Digitally signed by Sîrbu Ion
Date: 2026.01.12 10:20:15 EET
Reason: MoldSign Signature
Location: Moldova
MOLDOVA EUROPEANĂ

SPECIFICAŢII TEHNICE

Anexa nr. 22 la Documentația standard
aprobată prin Ordinul Ministrului Finanţelor nr. 115 din 15.09.2021

Numărul procedurii de achiziție: ***Licitație deschisă 21534414/ ocds-b3wdp1-MD-1767076219931***

Denumirea licitației: ***Servicii de mentenanță și dezvoltare a Sistemului informațional e-Dosar (gestiune electronică a cauzelor penale).***

Denumirea serviciilor	Denumirea modelului serviciului	Ţara de origine	Produ-cătorul	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 nr. 1 - Servicii de mentenanță și dezvoltare a Sistemului informațional e-Dosar (gestiune electronică a cauzelor penale).						
Servicii aferente mentenanței preventive (abonament).	----	MD	DSS	Specificațiile tehnice depline sunt descrise în cadrul Termenilor de Referință (TOR)	Conform cerintelor din Specificațiile tehnice depline descrise în cadrul Termenilor de Referință	**ISO**
Servicii aferente mentenanței adaptive (dezvoltare, tarif per oră).	----	MD	DSS	Specificațiile tehnice depline sunt descrise în cadrul Termenilor de Referință (TOR) Termeni de garanție minim 12 luni	Conform cerintelor din Specificațiile tehnice depline descrise în cadrul Termenilor de Referință (TOR) Specificațiile tehnice depline sunt descrise în cadrul Termenilor de Referință	
Servicii aferente mentenanței corective (dezvoltare, tarif per oră	----	MD	DSS	Specificațiile tehnice depline sunt descrise în cadrul Termenilor de Referință (TOR) Termeni de garanție minim 12 luni	Conform cerintelor din Specificațiile tehnice depline descrise în cadrul Termenilor de Referință	

Semnat:_____
Numele, Prenumele: Sîrbu Ion
În calitate de: Director
Ofertantul: DAAC Software Systems S.R.L.
Adresa: mun.Chisinau str.Calea Iesilor 10

OFERTA TEHNICĂ

privind serviciile de mentenanță și dezvoltare a Sistemului informațional e-Dosar
(gestiune electronică a cauzelor penale)

Descrierea serviciilor de mentenanță și dezvoltare a Sistemului informațional
e-Dosar (gestiune electronică a cauzelor penale)

I. ASPECTE GENERALE

1.1 Sistemul informatic supus mentenanței:

Serviciile de mentenanță achiziționate se referă Sistemului informațional „e-Dosar: Gestiune electronică a cauzelor penale"(în continuare – **e-dosar penal**), care presupune totalitatea de resurse şi tehnologii informaționale interdependente, metode şi personal, destinate înregistrării evenimentelor/acțiunilor, generării documentelor tipizate aferente proceselor penale, păstrării, prelucrării, furnizării şi utilizării informației privind cauzele penale, gestionării electronice a materialelor/documentelor asociate examinării cauzelor penale.

1.2 Descrierea sistemului informatic supus mentenanței

Din considerente de securitate descrierea detaliată a componentelor sistemelor informatice supuse mentenanței va fi prezentată după încheierea contractului de mentenanță.

Descrierea generică a acestuia este prezentată în continuare:

SIA E-dosar penal este resursă informațională de stat, destinată susținerii, prin fluxuri de lucru digitale, a activităților operaționale aferente proceselor penale, monitorizării executării deciziilor aplicate, inclusiv a celor cu efecte pe termen lung, furnizării de date către resursele informaționale de stat pentru evidența și statisticile infracțiunilor, precum și asigurarea suportului informațional organelor de urmărire penală, de constatare, și altor autorități cu competențe în examinarea cauzelor penale.

Sistemul urmează a fi integrat suplimentar cu Sistemului informațional automatizat „Registrul informației criminalistice şi criminologice"

SIA E-dosar penal este conceput și funcționează în conformitate cu prevederile următoarelor acte normative:

- Codul penal al Republicii Moldova nr. 985/2002;
- Codul de procedură penală al Republicii Moldova nr. 122/2003;
- Legea nr. 216/2003 cu privire la Sistemul informațional integrat automatizat de evidență a infracțiunilor, a cauzelor penale și a persoanelor care au săvârșit infracțiuni
- Hotărârea Guvernului nr.714/2024 pentru aprobarea Conceptului Sistemului informațional „e- Dosar: Gestiune electronica a cauzelor penale/contravenționale"
- Hotărârea Guvernului nr.267/2025 pentru aprobarea Regulamentului privind modul de ținere a resursei informaționale formate de Sistemul informațional „e-Dosar: Gestiune electronică a cauzelor penale/contravenționale" și modificarea punctului 38 din Conceptul-cadru al Sistemului informațional integrat al Ministerului Afacerilor Interne, aprobat prin Hotărârea Guvernului nr.147/2024

Posesorul SIA E-dosar penal este Ministerul Afacerilor Interne (MAI).

Deţinătorul SIA E-dosar penal este Serviciul Tehnologii Informaționale al MAI

Notă: Mentenanța se va efectua la toate modulele ale sistemului.

Sistemul automatizat informațional «e-Dosar» (în continuare – SIA «e-Dosar») este constituit dintr-un ansamblu de resurse și tehnologii informaționale, mijloace tehnice de program și metodologii, aflate în interconexiune și este destinat înregistrării, păstrării, prelucrării și utilizării informațiilor privind sesizările despre infracțiuni și cauzele penale instrumentate la faza urmăririi penale.

Sistemul oferă suport informațional pentru faza examinării sesizărilor cu privire la infracțiuni și faza urmăririi penale și furnizează informații relevante părților procesului penal.

În baza Sistemului se formează resursa informațională «Registrul infracțiunii «e-Dosar».

SIA «e-Dosar» reprezintă totalitatea sistematizată de date despre actele procedurale emise/întocmite de către organul de constatare în legătură depistarea unei infracțiuni și organul de urmărire, procuror sau judecătorul de instrucție în legătură cu examinarea sesizărilor cu privire la

infracțiuni sau în legătură cu efectuarea urmăririi penale, implicit plângerile, cererile, demersurile etc. depuse de persoanele interesate în desfășurarea procesului penal.

Sistemul informațional automatizat «eDosar» este destinat pentru a efectua procesele de

înregistrare, menținere și gestionare a datelor despre infracțiuni în structurile MAI (organele autorizate și subdiviziunile lor teritoriale și mobile).

Sistemul informațional automatizat «eDosar» asigură suport pentru ciclul de viață al dosarelor electronice privind examinarea sesizărilor cu privire la infracțiuni și dosarelor de urmărire penală: formarea dosarelor de proces penal, formarea dosarelor cauzelor penale, introducerea datelor și documentelor însoțitoare, prelucrarea, stocarea, și furnizarea informațiilor despre existența infracțiunilor și acțiunilor efectuate în legătură cu săvârșirea acestora, generarea datelor statistice.

SIA eDosar asigură următoarele sarcini funcționale:

a) Crearea unui dosar electronic al infracțiunii (proces penal/cauză penală)

− vizualizarea listei documentelor de inițiere pentru crearea unui dosar în cadrul procesului penal/cauzei penale (utilizatorul selectează documentul (ordonanță/proces-verbal) necesar);

− vizualizarea șablonului al documentului (ordonanță/proces-verbal) selectat (care inițiază crearea dosarului electronic);

− introducerea datelor în document (ordonanță/proces verbal);

− crearea automată a dosarului electronic pe baza documentului de inițiere;

− generarea automată a numărul unic (folosind un algoritm special) și atribuirea acestuia la dosarul electronic;

− încărcarea documentelor scanate sau a altor materiale necesare la dosar

b) Desemnarea unui grup de lucru

− vizualizarea de către conducător a listei dosarelor electronice noi create;

− căutarea (filtrarea) dosarelor de diverși parametri;

− vizualizarea fișei dosarului electronic (cu posibilitatea de a vizualiza documentele atașate);

− selectarea ofițeri de urmărire penală, numirea lor în grupul de lucru și numirea șefului grupei;

− notificarea angajatului despre numirea sa într-un grup de lucru;

− acordarea dreptului șefului grupei de a atribui dreptul de acces la altor angajați la dosarul electronic;

− acordarea automată a drepturilor de acces angajatului desemnat pentru dosarul curent

c) Managementul dosarului electronic

− vizualizarea listei dosarelor (restricționat conform drepturilor de acces)

− căutare dosarelor după diverși parametri;

− vizualizarea fișei dosarului electronic selectat;

− vizualizarea listei proceselor pentru procesul penal curent;

− vizualizarea listei cauzelor penale pentru cauzele penale curente;

− pentru proces penal/cauză penală selectat vizualizarea listei de documente, disponibile pentru acest proces/cauză;

− selectarea șablonului de document necesar și completarea acestuia;

− atașarea materialelor suplimentare (scanurilor, filmelor) la document;

− pentru a crea formularul statistic RICC, există anumite documente care trebuie să fie completate;

− aprobarea sau coordonarea documentelor conform ciclului lor de viața;

− vizualizarea listei documentelor, celor care sunt în dosar electronic cu indicarea statutului lor;

− luarea deciziei privind crearea unui dosar penal (în cadrul dosarului electronic curent)

− oferirea accesului instanțelor judecătorești și procuraturii la un dosar electronic (inclusiv cauză penală);

− oferirea instanțelor judecătorești și procuraturii posibilitatea de a atașa documentele la dosarul electronic;

− conexarea a două sau mai multe dosare electronice într-un singur dosar (cu numărul unic a dosarului electronic principal), lucrările ulterioare se desfășoară numai cu dosar electronic principal;

− disjungerea dosarelor electronice la dosarele constitutive (fără duplicarea documentelor create în dosar principal, fără posibilitatea selectării documentelor procesuale care vor fi transferate în dosarul electronic separat)

d) Gestionarea documentelor

− automatizarea ciclului de viață al documentelor în dependența de tipul acestora (schimbarea statutelor, condiții prealabile pentru crearea unui document);

− oferirea utilizatorilor șabloanelor de documente pentru completare;

− căutarea documentelor după procese, denumiri, date creării și vizualizării rezultatelor căutării;

− oferirea posibilității de a atașa copii scanate/filme video/foto la document;

− diferențierea accesului utilizatorilor la dosare electronice în dependența de rolul lor în sistem;

e) Evidența utilizatorilor

− evidența utilizatorilor conform afilierii lor la departamente (MAI, instanțele de judecată, procuraturii) și la subdiviziunile teritoriale;

− crearea fișei angajatului;

− evidența datelor de identificare;

− evidența datelor de contact;

− atribuirea rolurilor utilizatorilor și atribuirea drepturilor speciale;

− evidența cazurilor pe care le desfășoară angajatul;

− efectuarea căutării utilizatorilor după parametrii principali și vizualizarea rezultatelor căutării;

− actualizarea datelor angajaților;

− urmărirea utilizatorilor după statut;

f) Semnarea documentului cu semnătura electronică

− asigurarea aplicării semnăturii electronice pe documentul electronic;

− asigurarea aplicării semnăturii electronice pe fișierul în formatul Pdf;

− asigurarea verificării semnăturii electronice aplicate;

g) Funcțiile sistemului

− asigurarea utilizatorilor cu șabloane de documente;

− asigurarea ciclului de viață al documentelor cu vizualizarea statutelor acestora și posibilitatea luării unei decizii;

− urmărirea documentelor și a dosarelor electronice după statutul lor;

h) Monitorizarea funcționării sistemului și a utilizatorilor;

− salvarea istoricului statutelor a dosarului electronic;

− salvarea automată a informațiilor despre procesarea documentelor (cine, când, statutul);

− monitorizarea activității utilizatorilor din sistem;

i) Administrarea sistemului

- actualizarea clasificatoarelor/nomenclatoarelor;

− asigurarea cu mecanismul creării șablonului pentru introducerea datelor in documente în sistem;

− asigurarea cu mecanismul creării formelor de tipar pe suport de hârtie;

− înregistrarea utilizatorilor în sistem;

− gestionarea utilizatorilor, atribuirea rolurilor în dependința de nevoile funcționale;

− monitorizarea sistemului;

− configurarea sistemului.

Arhitectura sistemului informațional conține două niveluri:

a) nivel local (subdiviziuni teritoriale, instanțele de judecată, procuratura);

b) nivel central (oficiul central).

Baza de date, serverele care realizează business-logica și care oferă o interfață de utilizator sunt situate într-un singur loc la nivelul central.

Acces la sistem au doar utilizatorii înregistrați, cărora li se acordă drepturi în dependență de rolurile lor.

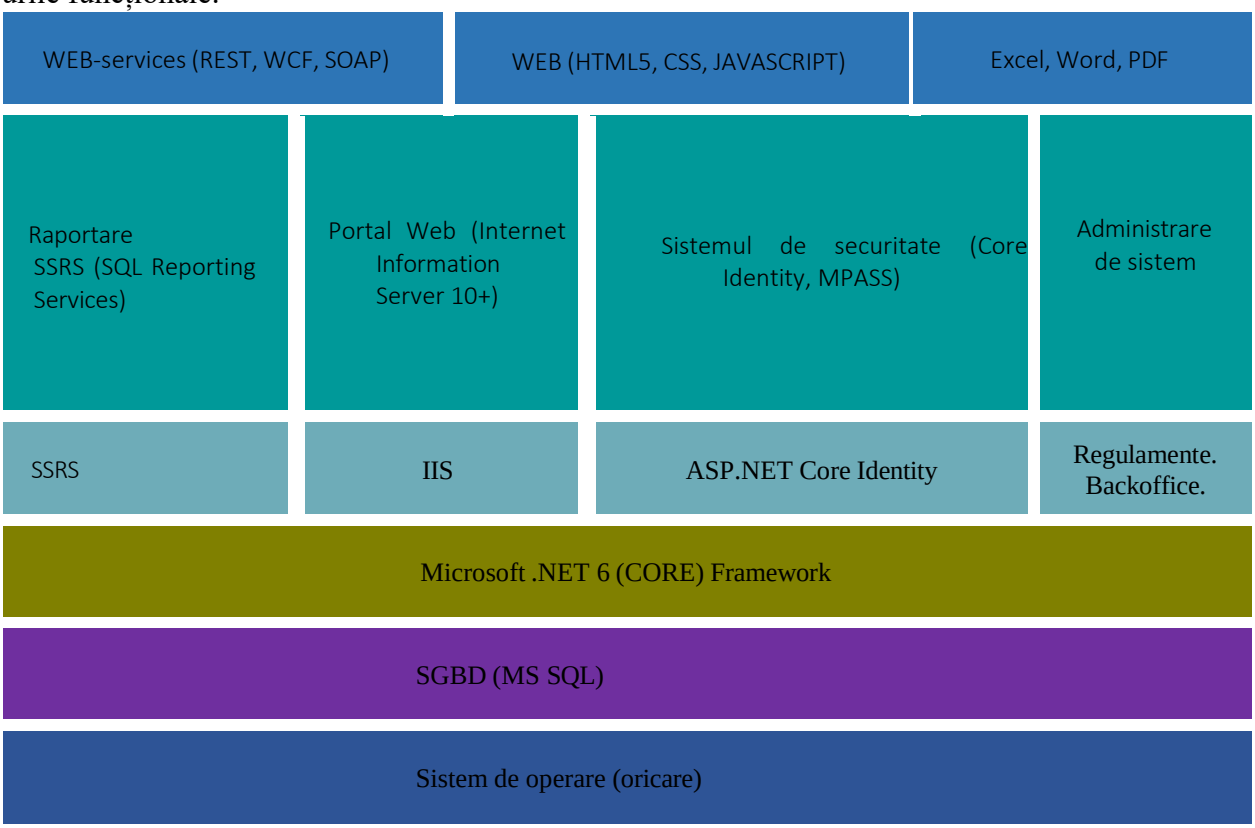
Interacțiunea utilizatorului cu sistemul se realizează utilizând interfața WEB.

Schimbul de informații între locurile de lucru ale utilizatorilor și serverele SIA se realizează în timp real prin Internet prin canale securizate.

Soluția se bazează pe platforma Microsoft .NET Framework, care este, de facto, standard industrial la elaborarea sistemelor informaționale multe niveluri și este susținut de cei mai importanți producători de software din lume.

Arhitectura software și hardware a soluției

Figura 1 demonstrează arhitectura software și hardware a soluției, ținând cont de componentele și blocurile funcționale.



ARHITECTURA SISTEMULUI „E-DOSAR”

Structural, sistemul „eDosar” este o soluție software care interacționează cu alte sisteme de informații prin intermediul serviciilor WEB și cu utilizatorii prin intermediul interfeței WEB.

Arhitectura sistemului „eDosar” permite dezvoltarea ulterioară a funcționalității.

Arhitectural, sistemul este o structură standard pe trei niveluri:

- BD
- server de aplicații (server de logică de afaceri)
- web client (server web, aplicații web)

precum și module de servicii web care oferă interacțiune cu sisteme de informații interne și externe.

Serverul de aplicații asigură executarea logicii principale de afaceri a sistemului și servește ca element de interacțiune între partea client și sistemele externe cu baza de date a sistemului.

Funcțional, serverul de aplicații este împărțit în 3 părți principale:

- sistem de securitate (gestionarea utilizatorilor, roluri, drepturi, activitate utilizator)
- sistem de înregistrare (înregistrarea acțiunilor utilizatorului și a evenimentelor din sistem)
- sistem de logică de afaceri (toate funcționalitățile de bază ale sistemului, gestionarea cazurilor, documentelor, cererilor de servicii web, asigurarea interacțiunii dintre partea client și baza de date)

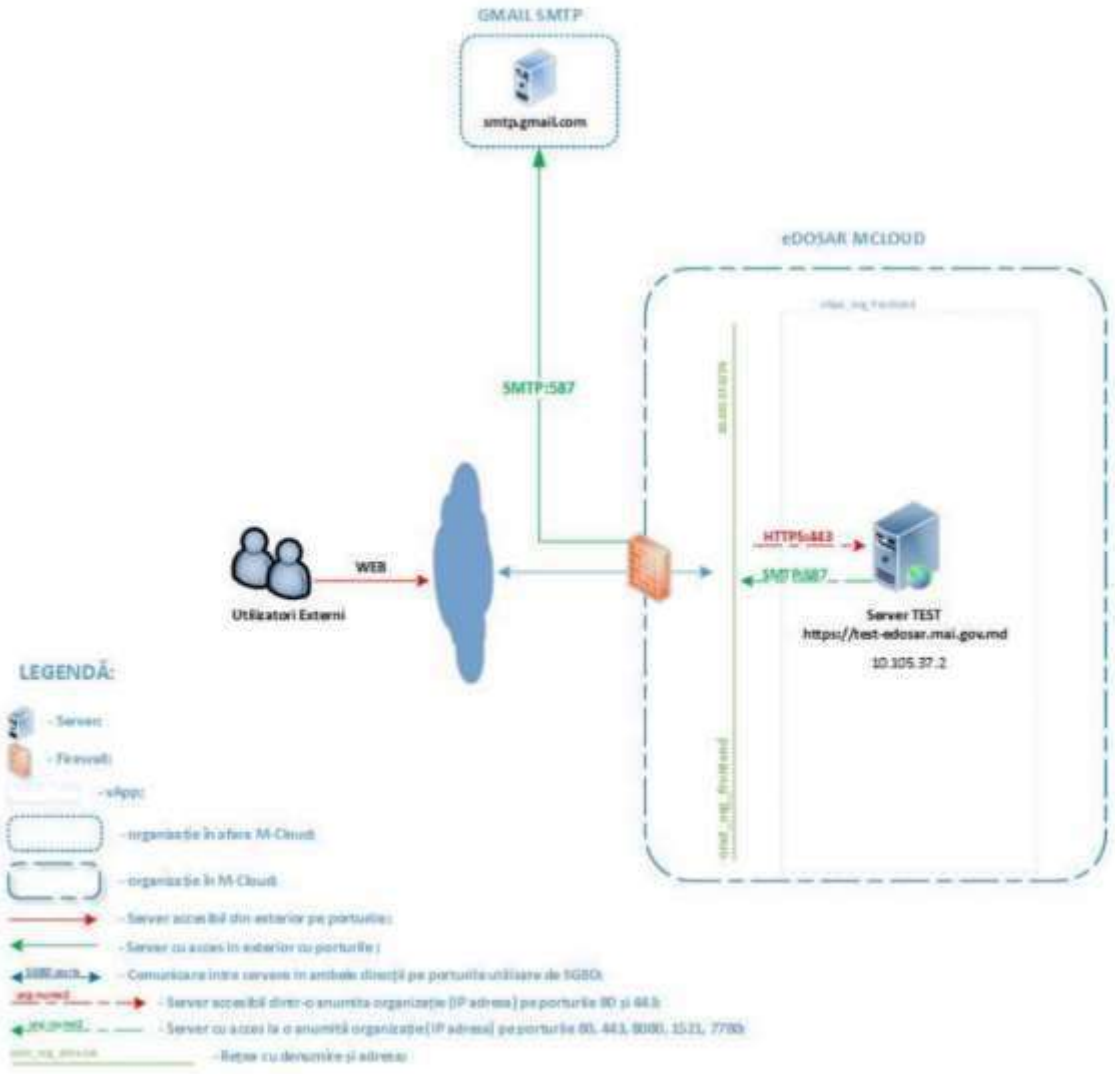
SIA „eDOSAR” este accesibila pe protocoalele HTTPS.

Platforma electronica este formata dintr-un server virtual:

• Server de TEST - bazat pe server web IIS 10 si SQL Server Developer 2019.

Serverul de aplicație (APP) are configurat certificat SSL, ceea ce permite de a proteja conexiunea dintre aplicație si utilizatorii finali.

Diagrama logică de conexiune a platformei sistemului „eDOSAR”



Roluri business în sistem

Principalele părți implicate la managementul dosarelor electronice sunt următoarele grupuri de utilizatori:

1. Reprezentanții organelor de constatare care au constatat o infracțiune au acces la procesele-verbale de constatare a infracțiunii până la remiterea acestora organului de urmărire penală;

2. ofițerii de urmărire penală și conducătorii subdiviziunilor de urmărire penală care gestionează procesul de examinare a proceselor penale/cauzelor penale, au acces la toate dosarele electronice, dar numai în limitele competenței lor;

3. membrii grupului de lucru care au acces numai la dosarele în care au fost desemnați (grupurile de lucru sunt entități temporare și sunt atribuite fiecărui dosar individual. Un angajat poate participa la mai multe grupuri de lucru în același timp);

4. angajații procuraturii și instanțelor de judecată care completează dosarele penale cu documentele necesare (dacă acești angajați nu sunt utilizatori ai sistemului, atunci documentele primite de la aceștia sunt introduse în dosar de către participanții gruplui de lucru);

5. administratorii susțin operabilitatea sistemului și nu au acces la dosare electronice.

№	Denumirea rolului business	Grup	Destinație în sistem și particularități
1.	Utilizator înregistrat	toate	Orice utilizator care a fost autentificat și identificat în sistem, căruia i s-au atribuit anumite drepturi (rol virtual)
2.	01. Registrator (reprezentant al organului de constatare sau ofițer de urmărire penală)	1	Angajat al MAI cu atribuții de constatare/depistare a infracțiunilor care **este împuternicit să creeze un dosar electronic nou** ***Notă:*** Registratorul are acces numai la etapa de creare a documentului inițial prin care poate fi creat un dosar electronic (proces-verbal cu privire la constatarea infracțiunii), în alte procese accesul la dosare îi este interzis.
3.	02.Ofițierul UP (OUP – membru al grupului de lucru)	1, 2	Ofițer împuternicit să desfășoare un proces penal/cauză penală de sine stătător sau în cadrul unui grup de urmărire penală, implicit să efectuează acțiuni de gestionare a documentelor dosarului (crearea documentelor/proceselor, introducerea datelor) ***Notă:*** are acces la datele și dosarele din gestiunea sa sau a celor în care a fost desemnat ca membru a grupului de urmărire penală.
4.	03.Conducătorul OUP	1	Conducător OUP, împuternicit să repartizeze ofițerilor de urmărire penală spre soluționare sesizările/materialele referitoare la săvârșirea infracțiunilor (procesele penale), precum și cauzele penale; să retragă materialele sau cauza de la un ofițer de urmărire penală și să le transmită altui ofițer pentru efectuarea urmăririi penale, cu posibilitatea întocmirii unei rezoluții direct în sistem; să dispună efectuarea urmăririi penale de către un grup de ofițeri de urmărire penală ; să înainteze procurorului demersuri cu privire la anularea unor acte juridice nelegitime ale ofițerului de urmărire penală; să își rețină sesizările (procesele penale), cauzele penale pentru efectuarea urmăriri penale, revenindu-i atribuțiile de ofițer de urmărire penală. ***Notă***: sunt disponibile datele și documentele din toate dosarele existente în subdiviziunea sa.
5.	05. Administrator de sistem	NC	Angajat al MAI care are drepturi speciale și îndeplinește funcții administrative și de supraveghere în sistem. ***Notă:*** administratorul de sistem nu are acces la datele dosarelor curente și arhivate.

6.	07.Procuror	3	Angajat al procuraturii împuternicit să conducă urmărirea penală; să efectueze acțiuni de urmărire penală și să atașeze documente la un anumit dosar electronic; aprobă documentele primite; anulează sau modifică documentele (actele procesuale) ilegale ale ofițerului de urmărire penală; retrage motivat dosarul (materialele/cauza penală) de la ofițerul de urmărire penală și îl preia în gestiune sau dispune transmiterea dosarului altui ofițer de urmărire penală; ordonă efectuarea urmăririi penale de către un grup de ofițeri de urmărire penală; decide excluderea probelor (documentelor) din dosar. Notă: dreptul de acces la dosar este acordat de către procurorul ierarhic superior, ofițerul de urmărire penală, după caz, șeful grupului de lucru (inclusiv pentru procuror sau judecător). După preluarea dosarului în exercitare personală de către procuror ofițerul de urmărire penală nu are acces la dosarul penal.
7.	08. Procuror ierarhic superior	3	Angajat al procuraturii cu atribuții de control asupra activității procurorului ierarhic inferior și ofițerului de urmărire penală, care este împuternicit să repartizeze către procurori dosarele pentru conducerea urmăririi penale; să efectuează personal acțiuni de urmărire penală; să adopte hotărâri și să aprobe documente; să anuleze, total ori parțial, să modifice sau să completeze actele procurorilor ierarhic inferiori și ale ofițerului de urmărire penală; să întocmească demersuri și indicații scrise; să atașeze sau să excludă documente din dosarul electronic; să ordone efectuarea urmăririi penale de un grup de procurori sau ofițeri de urmărire penală; să retragă motivat dosarul (materialele/cauza penală) de la procuror sau ofițerul de urmărire penală pentru a-l prelua în gestiune personală sau dispune transmiterea dosarului altui procuror/ofițer de urmărire penală; retrage dosarul de la un organ de urmărire penală și îl transmite organului de urmărire penală competent Notă: dreptul de acces la dosar este acordat din momentul începerii procesului penal/cauzei penale (crearea dosarului electronic). Dreptul de acces la dosar este acordat pentru procuror de către procurorul ierarhic superior, cu posibilitatea întocmirii unei rezoluții în sistem
8.	10. Judecător	3	Angajatul instanței judecătorești care are drept de vizualizare a documentelor care au fost prezentate de către procuror (bifate de procuror spre vizualizare) și după caz, atașează documente la un anumit dosarul electronic la care are acces. ***Notă:*** dreptul de acces la dosar pentru judecător este acordat de către procuror si prezuma concomitent marcarea/bifarea documentelor procesuale cu drept de vizualizare din dosar. La retragerea dreptului de acces pentru judecător se anulează acces spre vizualizare la toate documentele din dosar si la dosar.

9.	12. Șeful grupei de lucru (ȘG) - *numit din structura Ministerului Afacerilor Interne sau procuror*	2	Angajat al Organului de urmărire penală (MAI) sau procuror, care este desemnat in calitate de conducător a unui grup de lucru (grup de urmărire penală, ce poate fi compus din ofițeri de urmărire penala si procurori) pentru desfășurarea urmăririi penale a unui anumit dosar. Are drepturi de desemna(oferi acces la dosar) în grupul de lucru alți participanți, inclusiv cei din alte structuri (procuraturii, instanțe judiciare) și cei care efectuează acțiuni de gestionare a documentelor dosarului (creare proceselor/documentelor, introducere/modificare datelor) *Notă:* are acces la datele și dosarele, pentru care este atribuit grupului de lucru.

Obiectele de evidență

În sistem sunt următoarele obiecte de evidență. Principale:

a) Dosar electronic;
a) Proces penal (în cadrul dosarului electronic)
b) Cauză penală (în cadrul dosarului electronic)
c) Document (inclusiv formulare statistice RICC);
d) Copia scanată (orice fișier atașat);
e) Utilizator;

Suplimentare:

a) Subdiviziune (structurile Ministerului Afacerilor Interne, Procuraturii și instanțelor judecătorești);
b) Comunicarea;
c) Proces (proces penal/cauză penală)

INTEROPERABILITATEA CU ALTE SIA

Sistemul interacționează cu următoarele sisteme informaționale externe:

1. Serviciile MSign (eGov) – pentru aplicarea SE pe documente, de asemenea, pentru verificarea validității SE aplicate. Specificațiile tehnice sunt furnizate în conformitate cu cerințele serviciului MSign

2. Serviciile MPass (eGov) – pentru autentificarea utilizatorilor. Specificațiile tehnice sunt furnizate în conformitate cu cerințele serviciului MPass.

3. Serviciile MLog – pentru logarea în serviciul evenimentelor de sistem, care sunt jurnalizate în sistem.

4. Registrele de stat - recepționarea datelor din RSP, RSUD pentru completarea documentelor procesuale (prin MConnect)

5. SIA ”RICC” – colectarea datelor și crearea fișierelor JSON pentru completarea formelor statistice în RICC.

6. CUATM - în sistem va fi afișată lista de valori din clasificatorul unităților administrativ-teritoriale.

Interoperabilitatea este asigurata prin intermediul platformei guvernamentale de interoperabilitate ”MConnect”, prin utilizarea de web-servicii, în cadrul registrelor de stat al populației și unităților de drept.

Pe baza funcțiilor business și a scenarii de utilizare, sistemul are următoarea structură, care este prezentată în figură.

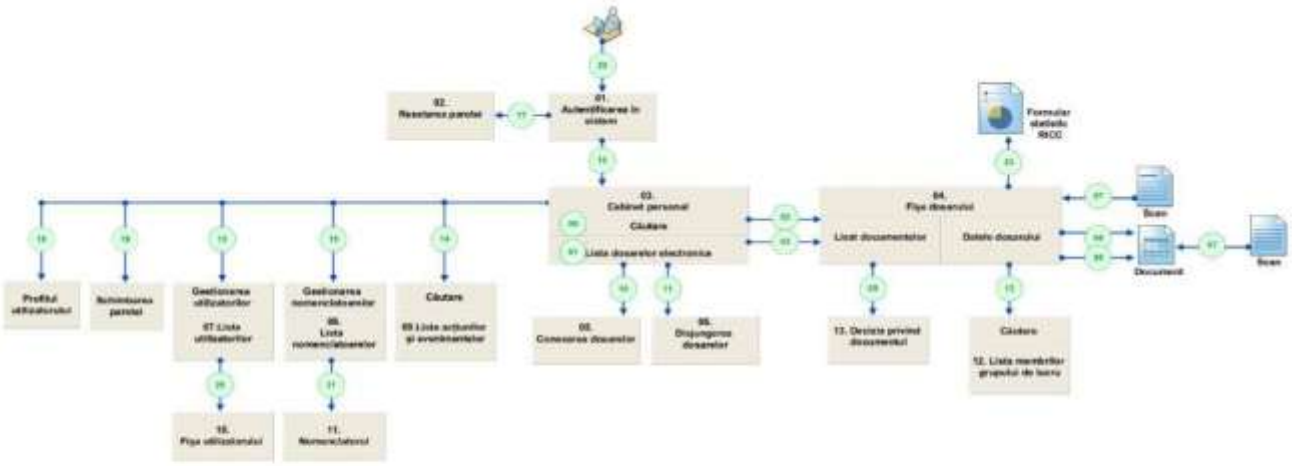


Figura 1 - Structura sistemului

Notă: cu culoarea verde în cercuri sunt marcate numerele funcții și funcții-business

Descrierea functiilor busines se va prezenta la solicitare

Obiectivul prezentelor cerințe este de a stabili regulile și procesele de interacțiune între Prestator și Beneficiar în vederea prestării și utilizării Serviciilor, nivelul agreat de Servicii, precum și responsabilitățile individuale ale Prestatorului și Beneficiarului în cadrul acestor procese, numite în continuare Servicii în vederea asigurării activităților, inclusiv în baza interpelărilor formulate de persoana responsabilă din partea Beneficiarului aferentă serviciilor prestate care presupun, dar nu se limitează la:

- Reinstalarea şi reconfigurarea componentelor de platformă libere (server web, server de baze de date, server de aplicaţii) şi a sistemului pe server propriu sau MCloud;
- Configurarea sistemului „la cheie” – configurarea, ajustarea şi introducerea opţiunilor şi nomenclatoarelor specifice instituției, importul nomenclatoarelor şi datelor din surse existente;
- Reinstalări şi reconfigurări ale sistemului, inclusiv ale componentelor de platformă libere şi open-source în versiuni actuale stabile;
- Actualizări periodice sau urgente, inclusiv în scopul eliminării vulnerabilităților, ale sistemului de operare şi ale componentelor de platformă (server web, server de baze de date, server de aplicaţii);
- Activităţi de suport tehnic;
- Activităţi de mentenanţă preventivă, adaptivă și corectivă;
- Actualizări ale sistemului, inclusiv instalarea versiunilor modernizate, în scopul ameliorării performanțelor şi uzabilităţii;
- Ajustarea sistemului, inclusiv revizuirea cerinţelor tehnice, la creşterea volumului de înregistrări şi a numărului de utilizatori;
- Consultarea utilizatorilor în probleme ce ţin de modul de funcţionare şi de condiţiile de exploatare a sistemului (prin telefon, e-mail, mesagerie, acces distant etc.);
- Acordarea asistenţei la administrarea bazei de date şi a clasificatoarelor şi nomenclatoarelor sistemului;
- Adaptarea funcţionalităţilor sistemului la condiţiile de utilizare ale instituţiei.

1. NOȚIUNI GENERALE

1.1 Termeni și definiții

În prezentul document se vor utiliza următorii termeni și definiții a lor:

Utilizator – orice persoana sau grup de persoane care folosește informația din sistemul informatic sau interacționează direct cu acesta.

Persoanele responsabile din partea beneficiarului – persoanele desemnate de Beneficiar care sunt în drept de a solicita de la Prestator oferirea serviciilor aferente obiectului achiziției și prin intermediul cărora Prestatorul comunică cu Beneficiarul. Persoanele responsabile din partea Beneficiarului dispun de competențe și drept de decizie privind solicitarea serviciilor conform prezentului contract.

Incident - este considerat orice eveniment neplanificat ce a afectat sau ar fi putut afecta disponibilitatea și indicatorii de performanță ai sistemului informatic.

Problemă – reprezintă cauza primară a apariției incidentelor.

Solicitare – orice interpelare din partea Beneficiarului aferentă sistemului informatic deservit.. Solicitările pot fi:

a) **Solicitare de suport** – reprezintă o solicitare a unui serviciu prevăzut expres de acordul de prestare servicii (SLA) privind funcționarea SIF sau/și mediului conex. În rezultatul solicitării de suport Beneficiarul așteaptă prestarea serviciului solicitat conform nivelului de calitate prestabilit.

b) **Incident** – reprezintă orice solicitare care are la bază un **incident** de funcționare a sistemului informatic. În rezultatul solicitării de suport Beneficiarul așteaptă o soluție privind înlăturarea sau ocolirea incidentului / problemei enunțate.

c) **Solicitare de dezvoltare** – orice solicitare care necesită dezvoltarea sistemului informatic și presupune realizarea de noi funcționalități prin elaborarea de cod program sau modificare conținut informațional a BD (bazei de date).

Nivelul serviciului – reprezintă nivelul agreat de Beneficiar al indicatorilor cantitativi care caracterizează calitatea funcționării serviciului (conform terminologiei internaționale Service Level Agrement).

Principiul "cel mai bun efort" – situație în care Prestatorul va depune toată diligența în vederea prestării Serviciilor la cea mai înaltă calitate posibilă dar fără a garanta conformarea la parametri de calitate prevăzuți în prezentele Reguli.

Orele de lucru – intervalul de timp cuprins intre orele 8:00 si 17:00, în zilele de lucru.

2. DESCRIEREA ȘI CONȚINUTUL SERVICIILOR

2.1 Definirea și documentarea planului de prestare a serviciilor (segmentul sistemelor deservite)

Serviciile de mentenanța vor fi prestate in conformitate cu reglementările tehnice prevăzute de "Procesele ciclului de viață al software-ului" RT 38370656 -002:2006.

2.2 Serviciile aferente mentenanței preventive

Serviciile aferente mentenanței de preventivă sunt orientate spre restabilirea funcționalității sistemului informatic, în caz de incident, în timp optim și cu un impact minim asupra activității operaționale.

Serviciile de mentenanță de corecție includ cel puțin activități*:

I. Activități aferente continuității sistemului informațional

I.01. Configurarea și gestionarea copiilor de rezervă

I.02. Verificarea integrității copiilor de rezervă și restabilirea, la necesitate, din copii de rezervă

I.03. Instalarea versiunilor noi ale sistemului informațional

II. Activități aferente asigurării securității informaționale a SI

II.01. Asigurarea, instalarea, gestionarea certificatelor SSL

II.02. Asigurarea configurărilor specifice privind transportul securizat de date (SSL)

II.03. Aplicarea și gestionarea mecanismelor de prevenire și detectare a intruziunilor în baza de signaturi (IPS/IDS)

II.04. Asigurarea securității mediului de găzduire, prin:

a) aplicarea și gestionarea regulilor de filtrare a traficului de rețea la nivel de mediu de găzduire;

b) aplicarea și gestionarea regulilor specifice de filtrare a traficului web;

c) aplicarea mecanismelor de protecție împotriva atacurilor DoS/DDoS;

III. Activități de monitorizare și suport tehnic

III.01. Soluționarea incidentelor

III.02. Monitorizarea disponibilității aplicației

III.03. Consultarea metodologică a beneficiarului

IV. Activități aferente documentației tehnice

IV.01. Menținerea actualizată a ghidului utilizatorului/administratorului

V. Activități aferente aplicației

V.01. Configurarea/ reconfigurarea nomenclatoarelor

V.02. Configurarea/ reconfigurarea categoriilor / subcategoriilor

V.03. Configurarea/ reconfigurarea registrelor / subregistrelor de evidență

V.04. Configurarea/ reconfigurarea parametrilor specifici ai aplicației

V.05. Configurarea/ reconfigurarea parametrilor de notificare

V.06. Înlăturarea erorilor de cod aferente aplicației

După caz, aceste activități presupun :

1. Managementul incidentelor:

a. Servici de linie fierbinte pentru gestiunea incidentelor: recepționarea, înregistrarea, analiza, clasificarea incidentelor, urmărirea procesului de soluționare și închiderea incidentului;

b. Excelarea și gestiunea incidentelor care dețin de funcțiile sistemului informatic, din numele Beneficiarului, pentru serviciile externalizare. Serviciile respective nu includ incidente legate de infrastructura TIC.

c. Corectarea erorii sau identificarea și aplicarea unei soluții de ocolire a acesteia;

d. Depanarea erorilor, formarea raportului de analiză și a recomandărilor;

e. Gestiunea jurnalului de incidente și raportare statistice privind incidentele;

f. Consultarea utilizatorului în aspecte ce dețin de incapacitatea acestora de utilizare a Sistemului informatic. Solicitările de consultanță sunt considerate incidente în cazul dacă determină incapacitatea utilizatorului de a utiliza funcționalul Sistemul informatic

2. Asistența administratorilor Beneficiarului la lucrările de restabilire a sistemului informatic.

3. Expertiza și documentarea detaliată a incidentelor.

4. Monitorizarea parametrilor de funcționare a sistemului.

Serviciul de mentenanță de avertizare (preventivă) este prestat în baza unei *Solicitări* intervenite drept rezultat al:

1. unui incident de funcționare a sistemului informatic;
2. solicitare de consultanță din partea utilizatorului în vederea accesării funcționalului supus mentenanței;
3. autosesizării intervenite în baza alertei sistemului de monitorizare.

Prestarea serviciilor se va efectua conform regulilor descrise în anexa nr.1.

2.3 Serviciile aferente mentenanței adaptive

Serviciile respective vor fi contractate per oră.

Serviciile respective intervin drept rezultat al unei *solicitări de dezvoltare* și sunt gestionate conform cerințelor descrise în anexa nr.1.

1. Analiza impactului modificărilor mediului (cadrul normativ legal, procesele de business, impactul modificării componentelor infrastructurii TIC, etc.) asupra sistemului informatic și formularea recomandărilor de dezvoltare a sistemului informatic;
2. Adaptarea componentelor sistemului informatic pentru migrarea pe alte platforme hardware, utilizarea a noi capacități de producere, etc.
3. Analiza parametrilor de funcționare a sistemului în vederea stabilirii suficienței performanță și formularea sarcinilor de optimizare / dezvoltare;
4. Analiza solicitărilor și definirea cerințelor de modificare. Consultarea Beneficiarului în vederea formularea sarcinilor de dezvoltare;
5. Consultare a Beneficiarului în aspecte ce deține de identificare, analiza și formularea sarcinilor de dezvoltare;
6. Analiza solicitărilor de dezvoltare formulate de Beneficiar și elaborarea Caietelor de Sarcină;
7. Consultare a Beneficiarului în aspecte de configurare a SO, SGBD și alte produse program care interacționează cu sistemul informatic;
8. Consultanță privind re-ingeneering, reconfigurare, optimizare (inclusiv virtualizarea componentelor funcționale) cu scopul înnoirii platformelor și tehnologiilor utilizate (inclusiv platforma mCloud).
9. Instruirea utilizatorilor și administratorilor sistemului.
10. Modificarea codului sursă conform noilor cerințe impuse de cadrul normativ sau mediul de producție.
11. Managementul schimbărilor:

a. Consultarea specialiștilor beneficiarului în vederea elaborării planurilor de implementare a modificărilor și suportul la implementarea acestora;
b. Analiza impactului, testarea și suportul privind aplicarea reînnoirilor pentru sistemele de operare, SGBD și alte componente program externe cu care interacționează sistemul informatic;
c. Testarea de comun cu specialiștii Beneficiarului a impactului modificărilor asupra parametrilor de funcționare și siguranței sistemului informatic;

12. Documentarea sistemului și lucrări de reinginerie ”inversă” (definirea structurii logice a în baza codului sursă).
13. Perfectarea scripturilor de corectare a datelor în vederea soluționării incidentelor legate de SIF.
14. Gestionarea documentației, inclusiv planul de continuitate aferente sistemului (segmentul sistemelor deservite).

2.4 Serviciile aferente mentenanței corective

Din serviciile ce se referă la mentenanță de corecție Beneficiarul va contracta doar servici de:

1. Consultare a Beneficiarului în aspecte ce deține de identificare, analiza și formularea sarcinilor de dezvoltare;
2. Analiza solicitărilor de dezvoltare formulate de Beneficiar și elaborarea Caietelor de Sarcini;

3. Consultare a Beneficiarului în aspecte de configurare a SO, SGBD și alte produse program care interacționează cu sistemul informatic;

4. Modificări ce țin de îmbunătățirea performanțelor, reducerea nivelului riscurilor;

5. Modernizarea arhitecturii.

6. Înlăturarea vulnerabilităților de sistem privind asigurarea disponibilității și integrării datelor.

Serviciile respective vor fi contractate per oră.

Serviciile respective intervin drept rezultat al unei *solicitări de dezvoltare* gestionate conform cerințelor descrise în anexa nr.1.

7. La realizarea activităților de ajustare/modificare a softului aplicativ pentru Sistemul informațional E-dosar penal se va asigura ca toate drepturile de proprietate intelectuală care decurg în temeiul Legii nr.230/2022 (referitor la „drepturile de autor și drepturile conexe"), inclusiv, dar fără a se limita la, drepturile de autor și drepturile conexe și alte subiecte de proprietate intelectuală create, produse și dezvoltate în conformitate cu acest document să fie predate prin acte de predare – primire (inclusiv codul-sursă pentru soft aplicativ) în numele STI/MAI pentru Sistemul informațional E-dosar penal - sunt transferate automat și considerat drept proprietate si intelectuala si de autor, exclusivă a STI/MAI, fără nicio taxă suplimentara și fără limitări in utilizare si dezvoltare/scalare a acesteia, fără drept de a fi transmise terțelor persoane (în afara Ministerului Afacerilor Interne și instituțiilor din subordinea acestuia).

3. NIVELUL SERVICIILOR

Serviciile de mentenanță prestate trebuie să asigure ficționarea sistemelor informatice la următorul nivel de servicii.

Nivelul de disponibilitate a Serviciilor stabilește timpul de funcționare/nefuncționare a Serviciilor prestate și nivelul de performanță garantată a acestora. Nivelul de disponibilitate a Serviciilor este definit de parametrii ce urmează:

1. Perioada garantată pentru disponibilitatea sistemelor informatice este: în zilele lucrătoare, interval de timp 08:00 – 17:00.

2. Nivelul garantat de disponibilitate a Serviciilor este de minim 99.50% mediu lunar. Criteriul determină că timp de o lună timpul total de indisponibilitate a sistemului informatic din cauza erorilor de cod nu poate depăși 3 ore.

3. Serviciile se consideră disponibile dacă, în perioada orelor de lucru, Beneficiarul va putea accesa Serviciile și utiliza funcționalitatea asigurată de Prestator. Timpul de răspuns la interpelările de accesare a Serviciilor nu trebuie să fie mai mare decât 1 secundă. Timpul de răspuns reprezintă intervalul maxim de timp în care sistemul informatic trebuie să răspundă la o solicitare de statut indiferent de nivelul de solicitare a acestuia. Timpul de răspuns nu specifică timpul în care utilizatorul va primi răspunsul la interpelarea sa.

4. În afara perioadei orelor de lucru, Prestatorul va asigura disponibilitatea Serviciilor în baza principiului "cel mai bun efort".

Anexa nr.1
Reguli privind organizarea și prestarea serviciilor

1. Scopul anexei

Scopul acestei Anexe este de a stabili regulile și procesele de interacțiune între Prestator și Beneficiar în vederea prestării și utilizării Serviciilor de mentenanță aferente Sistemuelor Informatice supuse mentenanței ale Beneficiarului, nivelul agreat de Servicii, precum și responsabilitățile individuale ale Prestatorului și Beneficiarului în cadrul acestor procese, numite în continuare Servicii.

Prezentele Reguli vor fi anexe la Contract și vor asigură cadrul funcțional pentru prestarea Serviciilor de către Prestator și utilizarea acestora de către Beneficiar.

2. Organizarea procesului de prestare a serviciilor

2.1 Interacțiunea între Părți

Aspectele administrative ce dețin de interacțiunea dintre Prestator și Beneficiar se va efectua prin intermediul Persoanelor responsabile desemnate de Părți.

Fiecare Parte va desemna câte o persoană responsabilă de relația cu cealaltă (Manager Suport Client). Părțile se vor informa reciproc, prin scrisoare oficială, despre persoana desemnată și informația de contact a acesteia (numele, prenumele, funcţia, nr. telefon, e-mail, etc.) în termen de maxim 3 zile de la semnarea Contractului. Schimbarea persoanei responsabile se va face conform aceleiași proceduri.

Suportul operațional la utilizarea Serviciilor este asigurat de către Prestator prin intermediul unui singur punct de acces - Serviciul Suport Clienți (SSC).

SSC al Prestatorului va fi disponibil 24x24x365 pentru recepționarea solicitărilor. Disponibilitatea pentru soluționarea acestora este determinată de nivelul agreat de servicii.

Prestatorul oferă Beneficiarului posibilitatea de a contacta SSC prin următoarele modalități (enumerate în ordinea descreșterii preferinței) :

1. utilizarea sistemului de gestiune a solicitărilor (Service Desk) al Prestatorului.
2. expedierea de e-mail la adresa SSC;
3. apel telefonic la numărul corporativ al SSC.

2.2 Reguli de înregistrare a solicitărilor

Solicitare este orice interpelare formulată de un utilizator al Beneficiarului aferentă sistemului informatic deservit. În funcție de natura evenimentului care a generat solicitarea și rezultatul așteptat, interpelarea poate fi clasificată drept:

a) **Solicitare de suport** – reprezintă o solicitare a unui serviciu prevăzut expres de acordul de prestare servicii privind funcționarea SIF sau/și mediului conex. În rezultatul solicitării de suport Beneficiarul așteaptă prestarea serviciului solicitat conform nivelului de calitate prestabilit. Serviciile de suport nu includ și nu prevăd dezvoltarea sistemului informatic dacă nu este stabilit altfel în acordul de prestare servicii de mentenanță.

b) **Incident** – reprezintă orice solicitare care are la bază un **incident** de funcționare a sistemului informatic. În rezultatul solicitării de suport Beneficiarul așteaptă o soluție privind înlăturarea sau ocolirea incidentului / problemei enunțate. Serviciile de suport nu includ și nu prevăd dezvoltarea sistemului informatic. În cazul când soluția optimă determină necesitatea de dezvoltare a sistemului informatic și există o soluție de ocolire a erorii care asigură funcționarea sistemului informatic la un

nivel de performanță acceptabil, atunci va fi aplicată soluția de ocolire, iar soluția optimă va fi recalificată în solicitare de dezvoltare.

c) **Solicitare de dezvoltare** – orice solicitare care necesită dezvoltarea sistemului informatic și presupune realizarea de noi funcționalități prin elaborarea de cod program sau modificare conținut informațional a BD (bazei de date). Serviciile de dezvoltare oferite de Prestator nu includ dezvoltare de funcțional care dețin de alte produse program utilizate de sistemul informatic sau licențele pentru acestea.

Orice solicitare din partea Beneficiarului este adresată Prestatorului prin intermediul SSC al acestuia.

În scopul enunțului solicitării către SSC al Prestatorului, Beneficiarul va întreprinde în ordinea indicată, următoarele:

1. Va consulta ghidurile utilizatorului în vederea asigurării corectitudinii acțiunilor sale și identificării eventualelor soluții;
2. Va consulta prin intermediul persoanei responsabile a Beneficiarului ”Baza de Cunoștințe” pusă la dispoziție de Prestator prin intermediul portalului intern al SSC;
3. Va contacta Serviciul Suport Clienți.

Beneficiarul trebuie să poată justifica modalitatea de contact selectată (ex. de ce apel telefonic și nu interfața web). Prestatorul poate solicita Beneficiarului să utilizeze altă modalitate de contactare a SSC, în cazul în care acest fapt corespunde Regulilor.

În scopul prestării serviciilor de mentenanță în care se încadrează solicitarea SSC:

1. SSC efectuează expertiza preventivă a fiecărei solicitări:
   - o identifică tipul acestuia: solicitare de suport, incident sau solicitare de dezvoltare:
   - o clasifică solicitările din punct de vedere al impactului și al urgenței declarată de Beneficiar.
   - o determinată prioritatea de soluționare considerând regulile privind managementul solicitărilor conform tipului acesteia.
2. Înregistrează informația necesară pentru acordarea suportului:
   - o *în cazul incidentelor*, identifică și înregistrează parametrii de mediu: componenta sistemului informatic la care se referă, consecutivitatea de acțiuni care au dus la apariția incidentului, conținutul incidentului, rezultatul așteptat, și alți parametri prevăzuți de reglementarea internă cu privire la gestiunea incidentelor.
   - o *în cazul solicitării de suport* identifică serviciul solicitat conform acordului;
   - o *în cazul solicitărilor de dezvoltare* înregistrează: conținutul solicitării, baza normativă pentru dezvoltare, descrierea succintă a business procesului necesar de dezvoltat și rezultatul așteptat.
3. Orice solicitare de dezvoltare parvenită în adresa Prestatorului va fi analizată de acesta și raportată decizia în termeni rezonabili dar nu mai mult de 15 zile lucrătoare, în funcție de complexitatea solicitării. Informarea oficială a Beneficiarului necesită să conțină::
   - o soluția – în cazul unor incidente/ probleme prezente în baza de cunoștințe sau repetitive.
   - o timpul necesar de prezentare a soluției – în cazul lipsei necesității investigării subiectului
   - o planul de analiză – în cazul necesității unor analize suplimentare
   - o refuzul sau redirecționarea sarcinii în cazul când aceasta nu deține de competența Prestatorului. În cazul refuzului Prestatorul va argumenta decizia și va comunica Beneficiarului în competența cui este soluționarea acesteia.
4. În cazul acceptării solicitării, Prestatorul va comunica soluția și va prezenta spre aprobare planul detailat de soluționare cu indicarea: timpului (om/ore), cu descrierea lucrărilor necesare de efectuat, necesarul de resurse, la necesitate inclusiv și din partea Beneficiarului, graficul de realizare a lucrărilor care va include proiectarea, elaborarea, testarea și darea în exploatare a soluției (software), și a costului estimativ conform tarifelor stabilite, cu descifrarea acestora pe activități ce urmează a fi întreprinse.

Planul de soluționare poate fi schimbat în funcție de evoluția soluției acesteia doar cu acordul ambelor părți.

5. Modul de realizare a activităților și prezentarea rezultatelor este determinat de tipul solicitării (incident / solicitare de suport / dezvoltare) și se va desfășura conform criteriilor descrise în continuare.

Orice solicitare și istoria prestării serviciului aferent este înregistrată de către SSC într-un sistem

de gestiune a solicitărilor (sistemul Service Desk). In acest scop, Prestatorul va oferi conturi de utilizator în sistemul Help Desk pentru a asigura monitoriza solicitărilor Beneficiarului;

3. Reguli privind Managementul incidentelor

Serviciile de suport sunt orientate soluționării incidentelor și problemelor de utilizare a sistemului informatic. Solicitările de consultanță sunt considerate de asemenea incidente în cazul dacă determină incapacitatea utilizatorului de a utiliza funcționalul sistemelor informatice supuse mentenanței.

3.1.1 Clasificarea incidentelor

Prestatorul și Beneficiarul vor conlucra strâns în vederea prevenirii incidentelor și în vederea soluționării operative a celor produse pentru a minimiza impactul acestora asupra utilizatorilor. Efortul și prioritatea acordată pentru soluționarea unui incident va ține cont de regulile stabilite la acest capitol. Impactul incidentului caracterizează consecințele acestuia asupra disponibilității și performanței sistemelor informatice supuse mentenanței. Urgența incidentului caracterizează operativitatea cu care acesta trebuie soluționat, pentru a minimiza impactul incidentului asupra Beneficiarului.

Prioritatea de escaladare și soluționare a incidentelor va fi în funcție de impactul și urgența incidentului. Algoritmul aplicat pentru stabilirea priorității unui incident este definit în continuare.

Tabelul 1. Stabilirea priorității de soluționare a incidentelor

		Impact		
		Înalt	*Mediu*	*Jos*
Urgență	***Înalt***	Critic	Înalt	Mediu
	Mediu	Înalt	Mediu	Jos
	Jos	Mediu	Jos	Neglijabil

Tabelul 2. Matricea de estimare a urgenţei incidentului

URGENȚĂ	**Descriere**
Înaltă	Un incident este estimat ca având nivelul urgenței ”Înalt” în una sau mai multe din următoarele cazuri: - pagubele provocate de incident cresc extrem de rapid; - există activități și operațiuni critice pentru afacerea Beneficiarului ce trebuie să fie efectuate imediat; - reacțiunea imediată poate preveni riscuri legale majore și de securitate (protecție) a informației.
Medie	Un incident este estimat ca având nivelul urgenței „Mediu” în una sau mai multe din următoarele cazuri: - pagubele provocate de incident cresc considerabil în timp; - există activități și operațiuni importante pentru afacerea Beneficiarului ce trebuie să fie efectuate imediat; - reacțiunea operativă poate preveni riscuri legale moderate și de securitate a informației.
Joasă	Un incident este estimat ca având nivelul urgenței ”Jos” în una sau mai multe din următoarele cazuri: - pagubele provocate de incident cresc relativ puțin în timp; - activitățile și operațiunile afectate nu trebuie continuate imediat; - nu există riscuri legale și de securitate a informației semnificative.

Tabelul 3. Matricea de evaluare a impactului incidentului

IMPACT	Descriere
Înalt	Un incident este estimat ca având nivelul impactului ”Înalt” în una sau mai multe din următoarele cazuri: - activitățile cheie ale Beneficiarului sunt întrerupte; - incidentul este vizibil din exteriorul organizației Beneficiarului și afectează utilizatori externi, reputația și imaginea Beneficiarului; - există riscuri legale și financiare majore pentru Beneficiar;
Mediu	Un incident este estimat ca având nivelul impactului ”Major” în una sau mai multe din următoarele cazuri: - activitățile importante ale Beneficiarului sunt întrerupte sau activitățile cheie sunt desfășurate cu dificultate; - incidentul a afectat utilizatori interni și un număr nesemnificativ de utilizatori externi; - există riscuri legale și financiare semnificative pentru Beneficiar;
Jos	Un incident este estimat ca având nivelul impactului ”Jos” în una sau mai multe din următoarele cazuri: - activitățile interne nesemnificative ale Beneficiarului sunt întrerupte, sau activitățile importante sunt desfășurate cu dificultate; - incidentul a afectat doar utilizatori interni ai Beneficiarului.

3.1.2 Raportarea și soluționarea incidentelor

Orice incident aferent Serviciilor este raportat de Beneficiar către SSC, conform procedurilor stabilite la capitolul 2.2 ”Reguli de înregistrare a solicitărilor”.

Prestatorul va reacționa la incidentele raportate de Beneficiar, conform regulilor din tabelul de mai jos. Regulile se aplică pentru perioada orelor de lucru. În afara orelor de lucru, soluționarea incidentelor se va baza pe principiul „cel mai bun efort”.

Prioritate incident	Timpul de reacție	Timpul de soluționare	Timp max. pentru corectare a cauzei*	Raportare primară
Critică	Timpul de reacție al Prestatorului – imediat;	până la 1 oră	8 ore	Telefon.
Înaltă	Timpul de reacție al Prestatorului – 15 minute;	3 ore	ora 12 a zilei următoare	Telefon; Sistem Service Desk
Medie	Timpul de reacție al Prestatorului – 4 ore;	24 ore	5 zile	Sistem Service Desk
Joasă	Timpul de reacție al Prestatorului – 24 ore;	3 zile	10 zile	Sistem Service Desk
Neglijabilă	Timpul de reacție al Prestatorului – 72 ore;	Cel mai bun efort.	-	Sistem Service Desk

***Notă:** se aplică pentru situația când soluționarea incidentului se face prin aplicarea unor măsuri de ocolire.

Prestatorului poate contacta persoana ce a raportat incidentul, pentru a preciza informația oferită de Beneficiar. De comun acord cu aceasta, Prestatorul poate revizui nivelul impactului și nivelul urgenței soluționării incidentului. Beneficiarul are de asemenea posibilitatea ca ulterior să revizuiască clasificarea stabilită inițial. Revizuirea poate fi necesară în funcție de progresele soluționării incidentului.

Prestatorul va diagnostica cauza incidentului și va identifica măsurile necesare a fi întreprinse pentru soluționarea incidentului. Pe tot parcursul soluționării incidentului, Prestatorul va oferi informația Beneficiarului privind progresele făcute în vederea soluționării incidentului.

Prestatorul pate solicita implicarea la gestiunea incidentului, a persoanelor responsabile ale

Beneficiarului. Conlucrarea este necesară în vederea diminuării impactului incidentului și soluționării operative a acestuia.

Un incident se consideră soluționat atunci când funcționalitatea este restabilită pentru Beneficiar, la nivelul stabilit conform prezentelor Reguli. În cazul în care Beneficiarul nu este de acord cu nivelul de soluționare a incidentului, poate solicita deschiderea repetată a incidentului. În caz contrar, incidentul se consideră închis.

Toate incidentele raportate de Beneficiar sunt înregistrate în cadrul SSC. Prestatorul încurajează Beneficiarul să raporteze orice incident sau suspiciune de incident. Acest fapt va permite îmbunătățirea continuă a nivelului Serviciilor prestate.

Îndată ce problema depistată va fi rezolvată, instalarea aplicaţiei modificate pe serverul de producţie va avea loc cu acordul Beneficiarului şi în baza unui plan de livrare coordonat.

3.1.3 Escaladarea incidentelor

În cazul în care un incident nu poate fi soluționat în timpul agreat, Părțile pot escalada incidentul la un nivel mai înalt de autoritate - către Managerul Suport Clienți. În ultimă instanță, pot fi formate grupuri de lucru specializate din partea Prestatorului și Beneficiarului, pentru a gestiona orice aspect ivit în relațiile dintre aceștia.

4. Reguli privind prestare a serviciilor de suport predefinite

4.1 Reguli de organizare a lucrărilor conform planului-grafic

Planul-program, cu indicarea termenilor de efectuare a lucrărilor de mentenanță este elaborat de Prestator și aprobat de Beneficiar în termen de 30 zile lucrătoare de la data intrării în vigoare a Contactului, conform analizei multilaterale efectuate de către Prestator a Sistemului Informațional E-dosar penal și a Planului de continuitate a SIA E-dosar penal, la necesitate inclusiv și cu angajații din partea Beneficiarului

Planul-program poate fi modificat în funcție de evoluția acestuia și apariția unor necesități de dezvoltare suplimentare în perioada contractuală cu acordul ambelor părți.

4.2 Reguli de asigurare a planului de restabilire

Procedurile de continuitate menite să asigure posibilitatea restabilirii disponibilității Sistemelor informatice în situații de incident vor fi implementate conform cerințelor din tabelul de mai jos.

Nr.	Categorie incident	Planul de restabilire	Timpul Obiectiv pentru Restabilire (TOR)	Momentul în Timp pentru Restabilirii (MTR) (pierderea de date admisă la momentul restabilirii)
1.	Căderea componentelor hard aferente Sistemului Informatic.	Ridicarea sistemului pe echipamentul din rezerva activă Sdandby.	TOR = 15 minute.	MTR = ultima tranzacție confirmată.
2.	Coruperea integrității datelor din bazele de date ale Sistemului Informatic.	Copii de rezervă incrementale la un interval de 15 minute.	TOR = 30 minute.	MTR = 15 minute.
3.	Alte incidente ce pot afecta disponibilitatea Sistemului Informatic.	Copii de rezervă conform punctelor 1 și 2 mai sus.	TOR = 2 ore.	MTR = 15 minute.

4.	Situații excepționale ce pot afecta disponibilitatea data centrului ce găzduiește infrastructura hard a Sistemului Informatic.	Copii de rezervă depline efectuate zilnic, stocate în afara data centrului de bază.	TOR = 3 zile.	MTR = 15 minute

Timpul Obiectiv pentru Restabilire specificat în tabelul de mai sus este valabil în perioada orelor de lucru. În cazul apariției situațiilor de incident ce au dus la pierderea datelor, Beneficiarul va restabili integral datele pierdute de la sursele din copiile de rezervă proprii.

Beneficiarul este responsabil pentru alocarea resurselor necesare organizării planului de restabilire.

5. Reguli privind prestare a serviciilor de dezvoltare

5.1 Solicitarea Serviciilor de dezvoltare

Solicitarea Serviciilor de dezvoltare se efectuează doar de Persoana autorizată din partea Beneficiari în baza unei solicitări conform regulilor descrise în capitolul 2.2 ”Reguli de înregistrare a solicitărilor”
În rezultatul analizei solicitării, Prestatorul va comunica planul de soluționare cu indicarea: timpului, lucrărilor necesare de efectuat, necesarul de resurse, inclusiv din partea Beneficiarului și a costului estimativ conform tarifelor.

5.2 Prestarea Serviciilor de dezvoltare

Prestarea serviciilor de dezvoltare se va efectua cu aplicarea următoarelor reguli:

a) Prestarea Serviciilor se efectuează exclusiv în baza planului aprobat de Beneficiar privind prestarea Serviciilor de dezvoltare. În caz de necesitate planul de soluționare poate fi modificat, cu acordul Părților, fapt menționat în noul plan, care va conține referința la planul inițial.

b) Un Serviciu de dezvoltare se consideră prestat în momentul confirmării acceptării soluției de către Persoana responsabilă din partea Beneficiarului.

c) Conform prevederilor Hotărârii Guvernului nr.677/2025 cu privire la consolidarea accesului la serviciile publice electronice în cadrul Portalului guvernamental integrat EVO utilizat la prestarea serviciilor publice electronice și aprobarea măsurilor necesare pentru implementarea modelului unitar de design, pentru sistem se aplică obligatoriu Modelul Unitar de Design (aprobat prin Ordinul directoarei AGE nr.3005-094 din 29 octombrie 2025) la toate etapele de proiectare, dezvoltare și actualizare a resurselor și sistemelor informaționale destinate prestării serviciilor publice electronice, inclusiv Prestatorul va asigura prezentarea informațiilor necesare spre coordonarea de catre Beneficiar a designul dezvoltat prin remiterea unei solicitări către AGE.

d) Termenul de prestare a Serviciului de dezvoltare include doar timpul necesar Prestatorului colectării informației, documentării, analizei și prestării nemijlocite a serviciului și poate fi diferit de intervalul de timp total dintre momentul enunțului acestuia și acceptării rezultatului, dar nu mai mult de 2 luni.

e) Neacceptarea rezultatului de către Beneficiar nu este considerat motiv pentru tarifare suplimentară sau modificarea planului de soluționare dacă n-au fost modificate condițiile inițiale ale solicitării (formularea problemei și rezultatul solicitat) sau dacă în procesul de analiză nu s-a identificat necesitatea efectuării unor lucrări suplimentare.

f) În cazul nealocări în termenii agreați a resurselor necesare din partea Beneficiarului termenul de soluționare se majorează cu timpul respectiv, aplicându-se după caz penalitățile prevăzute de contract.

g) Prestatorul va asigura executarea lucrărilor de elaborare a funcţionalităţilor suplimentare, în baza unor proceduri general recunoscute şi acceptate şi a standardelor agreate de Beneficiar, ţinând cont şi de ultimele cerinţe în materie de elaborare, şi calculate în baza tarifelor convenite de părţi.

h) Prestatorul, prealabil predării către Beneficiar, va asigura testarea funcţionalităţilor suplimentare (pe serverul de testare), conform cerințelor si condițiilor înaintate de Beneficiar, care se vor consemna prin proces-verbal. Pentru a testa funcţionalitatea suplimentară solicitată de Beneficiar,

acesta din urmă va asigura mediul software şi hardware, care va corespunde exact cu sistemul real şi va asigura acces liber Prestatorului, precum şi va oferi instrumente de testare necesare.

i) Prestatorul va prezenta pentru funcţionalităţile suplimentare realizate, următoarele livrabile care vor corespunde cerinţelor Ordinului nr. 78 din 01.06.2006 cu privire la aprobarea reglementării tehnice "Procesele ciclului de viaţă al software-ului" RT 38370656 -002:2006, inclusiv:

- Proiectul tehnic al sistemului actualizat (în limba română);
- Ghidul administratorului actualizat (în limba română)- actualizat;
- Ghidul utilizatorului (în limba română) - actualizat;
- Codul sursă actualizat (pe purtător magnetic – CD) în două exemplare, cu toate bibliotecile şi instrumentele necesare compilării componentelor sistemului;
- Actul de predare în exploatare industrială (în limba română).

i) Beneficiarul este în drept să verifice (testeze) funcționalitățile suplimentare ale sistemului, predate de către Prestator, în conformitate cu procedurile statuate în contract.

j) Integrarea funcționalităților suplimentare în sistemul real se va face doar de către specialiștii Beneficiarului, și/sau doar cu aprobarea acestora. Responsabilitatea pentru funcționarea sistemului real o va purta Beneficiarul.

k) Beneficiarul și Prestatorul se vor obliga să se informeze reciproc despre orice modificări aduse sistemului atît prin funcționalitățile suplimentare integrate, cît şi prin alte modificări cum ar fi dar fără a se limita la cele de administrare a sistemului (găzduire pe servere, adrese IP, resurse hardware alocate etc.

l) Prestatorul va transfera către Beneficiarul toate drepturile de proprietate intelectuală rezultate din contract, inclusiv asupra proiectelor, soluțiilor tehnice, codurilor sursă și executabilelor, livrabilelor, documentației, procedurilor, tichetelor/incidentelor gestionate prin aplicația de management al incidentelor, precum și asupra oricăror alte rezultate obținute în cadrul contractului. Toate drepturile patrimoniale de autor asupra operelor create în executarea contractului vor fi transferate către Beneficiar, cu excepția celor asupra cărora există drepturi de proprietate intelectuală preexistente. Orice rezultate sau drepturi, inclusiv drepturi de autor sau alte drepturi de proprietate intelectuală sau industrială, dobândite în cadrul contractului vor fi proprietatea exclusivă a Benmeficarului, care va avea dreptul de a utiliza, publica, cesiona sau transfera aceste drepturi fără restricții, cu excepția cazurilor în care există drepturi preexistente.

m) Informarea se va face în scopul excluderii unor lacune în comunicare ce va putea periclita buna funcționare a sistemului.

6. Alte cerințe și reguli privind prestarea serviciilor

6.1 Reguli față de procesul de aplicare a modificărilor

Prestatorul poate, la necesitate, implementa modificări de infrastructură sau funcționale aferente sistemelor informatice supuse mentenanței.

Fiecare acțiune de modificare a codului sursă, cu excepția celor urgente, neefectuarea imediată a cărora poate duce la indisponibilitatea Serviciilor sau poate afecta funcționarea acestora, va fi coordonată în prealabil cu Beneficiarul..

1. Pentru fiecare lucrare de modificare va fi elaborat planul de aplicare a modificărilor care va include:

1. Descrierea modificărilor aplicate și componentele afectate.
2. Planul detaliat de efectuare a lucrărilor cu indicare: termenilor, consecutivitatea, acțiunile și persoanelor responsabile, lista și locația versiunilor noi, planul de efectuare a copiilor de rezervă, activitățile de testare a succesului aplicării modificărilor.
3. Planul de rezervă în caz de insucces care conține algoritmul de revenire la versiunea anterioare, restabilirea sistemului informatica din backup, sau soluție alternativă de asigurare a disponibilității serviciilor pe perioada soluționării incidentului.

Aceste modificări pot necesita testarea prealabilă implementării în mediul de producție. Prestatorul va notifica cu 5 zile în avans despre necesitatea efectuării testelor în mediul de testare și va comunica Planul de testare Beneficiarului

Beneficiarul este responsabil să participe la testele inițiate de Prestator, conform Planului de

testare.

Pentru menținerea nivelului agreat al Serviciilor, Prestatorul va efectua lucrări de modificare a sistemului informatic. Tipul lucrărilor de respective și angajamentele Prestatorului privind notificarea Beneficiarului, perioada și durata acestora sunt stabilite în tabelul de mai jos.

Tipul lucrărilor	Notificare Beneficiar	Condiții de inițiere	Perioadă și durată lucrări
Modificări minore ce nu influențează nivelul serviciilor	Cu 1 zi în prealabil.	Planul de aplicare a modificărilor aprobat de Beneficiar Prezența specialiștilor cheie ce asigură administrarea componentelor sistemului informatic	Sunt efectuate în afara orelor de lucru. Durata acestor lucrări nu va depăși 4 ore.
Modificări majore ce necesită oprirea integră sau parțială a sistemului	Cu 3 zile în prealabil.	Planul de aplicare a modificărilor aprobat de Beneficiar. Raportul de testare aprobat de Beneficiar.	Sunt efectuate în afara orelor de lucru. Durata acestor lucrări nu va depăși 24 ore.
informatic sau implică riscuri de funcționare a acestuia		Prezența specialiștilor cheie ce asigură administrarea componentelor sistemului informatic.	
Lucrări urgente, neefectuarea imediată a cărora poate duce la indisponibilitatea Serviciilor sau poate afecta funcționarea acestora.	Cu notificarea imediat ce a apărut necesitatea inițierii lor.	Prezența specialiștilor cheie ce asigură administrarea componentelor sistemului informatic.	Pot fi efectuate în orice perioadă. Durata acestora nu va depăși 2 ore. Toate acțiunile și deciziile întreprinse vor fi comunicate Beneficiarului.

Lucrările de aplicare a modificărilor vor fi efectuate de către Prestator cu impact minim asupra parametrilor de funcționalitate și disponibilitate a Serviciilor.

În cazul apariției neconcordanței specificației funcționale, Prestatorul se obligă să notifice în scris cu prezentarea descrierii detaliate a soluțiilor pentru înlăturarea neconcordanței.

6.2 Documentația tehnică

Prestatorul menține în stare actuală documentația tehnică aferentă sistemelor informatice. Documentația conține suficientă informație pentru ca orice echipa de dezvoltatori soft /administratori terți să poată prelua serviciile de mentenanță.

Prestatorul va notifica Beneficiarul despre noile versiuni și modificările importante, la documentația tehnică aferentă sistemelor informatice destinată Beneficiarului.

6.3 Mediul de test

Pentru efectuarea testărilor funcționale a Sistemului Informatic supus mentenanței, Prestatorul pune la dispoziția Beneficiarului un mediu de test. Mediul de test va putea fi utilizat de Beneficiar în următoarele cazuri:

- La apariția unor probleme semnificative în mediul de producție. În aceste situații, utilizarea mediului de testare poate fi solicitată atât de Beneficiar, cât și de Prestator;
- La implementarea modificărilor importante pentru sistemele informatice supuse mentenanței și testarea lor prealabilă pe mediul de test

Accesarea sistemelor informatice în mediul de testare se face în bază de canale securizate prin autentificarea similară cu mediul de producție.

6.4 Soluționarea divergențelor

Orice divergențe ivite între Părți vor fi soluționate cu efort comun și prin strânsă conlucrare între Părți. În acest scop, vor fi aplicate următoarele reguli:

1) Părțile vor forma un grup comun de lucru în scopul soluționării divergențelor. De comun

acord, în grupul de lucru pot fi acceptați reprezentanți ai părților terțe, inclusiv: experți independenți.

2) La necesitate, părțile vor pregăti probele electronice relevante pentru aspectele ce au devenit obiect de divergență.

3) Grupul de lucru se va convoca și va examina subiectul divergențelor și probele existente la subiect. Părțile vor aplica prevederile Contractului și prezentele Reguli în scopul clarificării tuturor aspectelor disputate și identificării unei soluții echitabile pentru divergențele ivite. În acest scop, pot fi ascultate, sau obținute în scris, opiniile membrilor externi, convocați în grupul de lucru, precum și rezultatele de expertiză ale probelor electronice existente.

4) Concluzia grupului de lucru va fi fixată în baza unui proces - verbal, semnat de membrii grupului de lucru din partea ambelor părți.

Identificarea unei soluții echitabile pentru ambele Părți, în limite angajamentelor asumate ale Părților, este preferabilă în toate situațiile de divergență. În cazul în care o asemenea soluție nu poate fi identificată, părțile vor aplica prevederile Contractului pentru soluționarea litigiilor.

6.5 Raportarea privind nivelul serviciilor

Părțile vor opta pentru prestarea transparentă a Serviciilor. În acest scop, Prestatorul va prezenta cu regularitate Beneficiarului rapoarte privind conținutul și nivelul Serviciilor acordate. Beneficiarul va formula propuneri privind conținutul rapoartelor de monitorizare a serviciilor. Structura rapoartelor respective este stabilită de Prestator.

Rapoartele prezentate, regularitatea și modalitatea de prezentare a acestora, este stabilită în tabelul de mai jos.

Tip raport	Conținut	Destinație	Regularitatea
Raport privind volumul serviciilor	Tipul solicitării, durata soluționării și tarifele aplicate.	Raportul este prezentat în scopul asigurării transparenței privind prestarea Serviciilor la nivelul agreat de Prestator.	Lunar, în formă electronică. La solicitarea Beneficiarului, pe suport de hârtie.
Raport privind solicitările de modificare	Propunerile de modificare a Serviciilor	Raportul este prezentat în scopul asigurării transparenței dezvoltării SIF.	Lunar, în formă electronică. La solicitarea Beneficiarului, pe suport de hârtie.
Raport privind nivelul serviciilor.	Nivelul de disponibilitate a sistemului, întreruperi planificate, incidente raportate, solicitări de suport.	Raportul este prezentat în scopul asigurării transparenței privind prestarea serviciilor la nivelul agreat de Prestator.	Lunar, în formă electronică, disponibil în Sistemul Service Desk. La solicitarea Beneficiarului, pe suport de hârtie.

6.6 Securitatea informației

Părțile agreează de comun acord să conlucreze și să coopereze în vederea gestiunii proactive a riscurilor de securitate a informației ce pot afecta serviciile Prestatorului și sistemele Beneficiarului, dependente de serviciile Prestatorului.

Prestatorul este responsabil pentru securitatea tehnologică și funcțională a sistemelor informatice supuse mentenanței, în limitele sarcinilor de mentenanță îndeplinite.

Beneficiarul este responsabil pentru utilizarea securizată a serviciilor oferite de Prestator.

În cazul unui incident de securitate a informației, partea ce a constatat incidentul va notifica imediat și cealaltă parte, dacă aceasta poate fi de asemenea afectată de incident. Părțile vor coordona măsurile necesar a fi întreprinse în scopul diminuării impactului incidentului și soluționării acestuia.

La solicitarea Beneficiarului, Presatorul va întreprinde acțiunile de rigoare în scopul colectării și conservării probelor ce pot fi necesare la investigarea incidentului și la probarea juridică a responsabilității pentru incident. În acest scop, Prestatorul, la solicitarea Beneficiarului, poate efectua:

- Colectarea și conservarea fișierelor log ce conțin informația privind accesul la nivelul componentelor de rețea;
- Efectuarea copiilor de rezervă depline pentru sistemele informatice supuse mentenanței, stocarea acestora în condiții ce asigură integritatea copiilor de rezervă efectuate;

- Întocmirea proceselor - verbale cu participarea a cel puțin 3 specialiști din partea Prestatorului, privind efectuarea copiilor de rezervă. Prezența reprezentanților Beneficiarului este solicitată;
- Menținerea formală a Registrului privind deținerea probelor conservate (chain of custody).

După soluționarea unui incident de securitate, părțile vor întocmi rapoarte individuale privind gestiunea incidentului. De comun acord vor întocmi un plan de acțiuni pentru prevenirea repetării incidentelor similare.

7. Descrierea generală a Serviciului ServiceDesk al companiei

Pentru asigurarea executării eficiente a serviciilor de suport în cadrul Departamentului de Asistență și Mentenanță este folosit serviciul automatizat de suport tehnic (ServiceDesk) pe baza standardelor IT Infrastructure Library (ITIL) și a managementului calității serviciilor IT (IT Service Management — ITSM). Metodologia ITIL, recunoscută în întreaga lume, de structurare a serviciului de suport tehnic, descrie cele mai bune metode practice de organizare a lucrului și interacțiunii subdiviziunilor IT ale companiei.

Avantajele soluției bazate pe ITIL/ITSM:

- oferirea de servicii IT devine mai orientată înspre client, acordul cu privire la calitatea serviciilor contribuie la îmbunătățirea relațiilor;
- serviciile sunt descrise mai bine, în limba clientului și cu detalierea necesară;
- sunt mai bine controlate calitatea și costul serviciilor;
- este îmbunătățită relația reciprocă între client și executor;

Serviciul Service Desk implementat în cadrul companiei noastre îndeplinește funcțiile de recepționare și procesare a adresărilor, incidentelor, cererilor de asistență, plângerilor, cererilor de modificare, precum și de analiză și interpretare ulterioară a acestora.

7.1 Avantajele Service Desk

Punct unic de intrare pentru clienți – toate cererile parvin la un telefon unic cu multiple canale sau la o adresă electronică unică

Simplificarea restabilirii operațiilor normale de acordare a serviciilor cu daune minime pentru clienți în limitele nivelului convenit de servicii și a priorităților businessului

Orice cerere, transmisă prin Service Desk trece prin următoarele etape:

1. primirea cererii, prima linie de interacțiune cu clienții
2. înregistrarea incidentului sau a cererii de asistență
3. realizarea evaluării inițiale a adresării, încercarea de a o soluționa sau de a determina, cine este în stare de a o soluționa
4. desemnarea inginerului, responsabil de soluționarea problemei
5. identificarea problemei
6. soluționarea problemei
7. determinarea necesității de instruire a clienților
8. închiderea incidentului și înștiințarea clientului

Informarea clienților despre starea și procesul cererii acestora are loc la toate etapele schimbării statutului acesteia în decursul procesării de la depunere și până la închidere.

1. Depunerea cererilor de asistență și executarea acestora.

   Timpul acordării serviciilor: de luni până vineri de la 08:00 până la 18:00, excluzând zilele sărbătorilor naționale, stabilite de guvernul Republicii Moldova.
2. Depunerea cererilor are loc prin solicitare scrisă, expediată la adresa poștei electronice servicedesk@daac-system.com, sau prin fax +373-22-509-710. În cazuri extreme, cererea poate fi adresată la numărul de telefon +373-22-509777. Confirmarea scrisă a cererii adresate prin telefon, este obligatorie.
3. În cerere trebuie să fie comunicat:
   - Numărul de contact
   - numele, prenumele și funcția persoanei care a depus cererea
   - denumirea echipamentului defectat și numărul de serie al acestuia
   - locul amplasării echipamentului
   - semnele defecțiunii (defectului)

Operatorul ServiceDesk realizează:

1. Primirea adresărilor utilizatorilor prin telefon și poșta electronică.
2. Înregistrarea adresărilor în sistemul ServiceDesk.
3. Analiza primară a adresării.
4. Transmiterea problemei către prima linie de suport.

Inginerul primei linii de suport realizează:

1. Diagnosticul la distanță.
2. Acordarea de asistență utilizatorului în soluționarea problemei sau oferirea de suport necesar, inclusiv consultarea prin telefon.

3. Încercarea de soluționare a chestiunii prin acces de la distanță.
4. Transmiterea adresărilor la alte niveluri de suport.

În cazul imposibilității soluționării problemei la distanță, șeful serviciului de suport desemnează inginerul responsabil și este luată decizia cu privire la deplasarea acestuia la locul amplasării echipamentului.

Sosirea inginerului la locul amplasării echipamentului are loc cel târziu în ziua lucrătoare următoare.

În caz de necesitate, problema este transmisă la alte niveluri, până la serviciul de suport tehnic al producătorului respectiv.

În caz de necesitate vor fi conectate toate resursele necesare ale companiei, suficiente pentru soluționarea problemei parvenite.