

Caiet de sarcini

Servicii de mentenanță, suport tehnic și administrare

Sistemul Informațional Automatizat Consul

Sistemul Informațional de Gestionare a Vizelor

1. Scopul general

Asigurarea funcționării continue, eficiente și sigure a Sistemului Informațional Automatizat Consul (SIAC) și Sistemului Informațional de Gestionare a Vizelor (SIGV), inclusiv suport tehnic, mentenanță, administrare tehnică și securitate cibernetică, în vederea susținerii activităților Ministerului Afacerilor Externe (MAE) și ale Misiunilor Diplomatice și Oficiilor Consulare (MDOC).

2. Obiective

Prestatorul va asigura:

- disponibilitatea și funcționarea continuă a sistemului;
- suport tehnic prompt pentru utilizatori și administratori;
- menținerea securității cibernetice și operaționale a sistemului;
- monitorizarea permanentă a infrastructurii și aplicației;
- remedierea rapidă a incidentelor tehnice;
- optimizarea funcționării sistemului.

3. Structura serviciilor de mentenanță

3.1. Servicii de mentenanță preventivă

Servicii planificate, executate periodic, destinate menținerii funcționării optime a sistemelor informatice:

- monitorizare infrastructură și aplicații;
- actualizări software și patch-uri de securitate;
- verificări periodice (backup, loguri, performanță);
- optimizări și mentenanță proactivă.

3.2. Servicii de mentenanță corectivă

Servicii de intervenție pentru remedierea incidentelor și disfuncționalităților apărute:

- diagnosticare și remediere incidente;
- suport tehnic utilizatori;
- restabilire funcționalitate servicii;
- intervenții de urgență.

3.3. Servicii de mentenanță adaptivă

Servicii necesare adaptării sistemelor informatice la modificări de mediu, cerințe sau integrare:

- modificări de configurații;

- adaptări la schimbări legislative / organizaționale;
- integrare cu alte sisteme;
- ajustări funcționale minore.

4. Gestionare și mentenanță tehnică

Prestatorul va asigura:

- supravegherea permanentă a funcționării sistemului;
- monitorizarea componentelor sistemului de operare și software;
- identificarea și remedierea incidentelor;
- restabilirea funcționalității sistemului în regim de urgență;
- gestionarea actualizărilor tehnice ale sistemului de operare și aplicației;
- gestionarea bazelor de date și a serviciilor aplicației;
- menținerea integrității și disponibilității datelor.

5. Suport tehnic și punct unic de contact

Prestatorul va asigura:

- un punct unic de contact (Single Point of Contact) disponibil 24/7;
- raportarea incidentelor prin telefon, e-mail sau sistem de ticketing;
- informarea utilizatorilor privind progresul soluționării incidentelor;
- mecanism standardizat de escaladare a incidentelor;
- sistem de ticketing pentru evidența solicitărilor.
- instalarea și configurarea stațiilor grafice - de preluare a datelor biometrice;
- asistență și consultanță în procesul de utilizare a sistemelor și a echipamentului de preluare a datelor biometrice.

6. Mentenanță corectivă

Mentenanța corectivă include:

- diagnosticarea incidentelor raportate;
- remedierea erorilor software;
- corectarea bug-urilor;
- rezolvarea problemelor de integrare cu sisteme externe (MPass, MPay, MSign, Agenția Servicii Publice, AccesWeb, Biroul Migrație și Azil, Inspectoratul General al Poliției de Frontieră etc.);
- aplicarea patch-urilor urgente;
- testarea regresivă după remedierea incidentelor.

Scopul este reducerea timpului de indisponibilitate a sistemului și menținerea continuității serviciilor consulare.

7. Mentenanță preventivă

Mentenanța preventivă include:

- aplicarea patch-urilor de securitate;
- actualizarea componentelor software;
- verificarea periodică a integrității bazelor de date;
- verificarea mecanismelor de backup;
- monitorizarea performanței sistemului;
- generarea semestrială a rapoartelor de sănătate ale sistemului.

8. Mentenanță adaptivă

Mentenanța adaptivă include:

- Crearea și asigurarea interacțiunii/interoperabilității cu sistemele informaționale ale Agenției Servicii Publice, Inspectoratului General pentru Migrațiune, Inspectoratului General al Poliției de Frontieră, Serviciul de Informații și Securitate).
- Oferirea posibilității funcționarului consular de modificare a datelor din dosarul depus de către solicitant.
- Oferirea posibilității MAE de a atașa documente adiționale la dosar, la etapa inițială și/sau după avizare sau declararea admisibilității dosarului.
- Crearea posibilității rechemării/retragerii dosarului de viză de la avizare la Inspectoratul General pentru Migrațiune
- Crearea posibilității vizualizării în sistem a persoanei care a examinat dosarul de viză.
- Modificarea paginii evisa.gov.md (front page): structură și conținut.
- Ajustarea informației la momentul emiterii unui aviz negativ de către IGM, informația introdusă de IGM la câmpul Note operator să fie automat transmisă în mesajul expedit la adresa de email a solicitantului.
- Dacă data valabilității documentului de călătorie a solicitantului este mai puțin de 3 luni de la data intrării în Republica Moldova, sistemul să nu-i permită să meargă la pasul următor.
- Crearea posibilității rechemării dosarului de viză de la avizare, cu mențiunea „a fost expedit eronat”.

9. Backup și continuitatea serviciilor

Prestatorul va asigura:

- realizarea copiilor de rezervă pentru sistem, baze de date și cod;
- verificarea periodică a integrității backup-urilor;
- testarea procedurilor de restaurare;
- documentarea procedurilor de Disaster Recovery;
- restabilirea funcționării sistemului în caz de incident major.

10. Niveluri de servicii (SLA)

Prestatorul va asigura funcționarea continuă a sistemului și suportul tehnic conform următorilor indicatori minimi de performanță:

Disponibilitatea minimă a sistemelor: 99% lunar, excluzând ferestrele planificate de mentenanță.

Clasificarea incidentelor

Nivel	Descriere	Timp reacție	Timp remediere
Critic	Sistem indisponibil total	30 min	2 ore
Major	Funcționalitate esențială afectată	1 oră	4 ore
Minor	Probleme necritice	4 ore	24 ore

Prestatorul va prezenta **rapoarte lunare SLA**.

11. Securitate cibernetică

Prestatorul va asigura:

- aplicarea patch-urilor de securitate;
- monitorizarea vulnerabilităților;
- configurarea firewall-urilor;
- accesul exclusiv de la adrese IP autorizate și documentate.
- prevenirea accesului neautorizat;
- monitorizarea accesului la sistem;
- auditarea periodică, cel puțin semestrial a logurilor.

12. Controlul accesului și autentificare

Prestatorul va asigura:

- autentificarea utilizatorilor prin MPass;
- utilizarea parolelor doar în situații excepționale;
- parole complexe (minim 8 caractere);
- blocarea conturilor după încercări nereușite de autentificare;
- schimbarea periodică a parolelor, cel puțin odată la 3 luni.

13. Controlul accesului administrativ

Prestatorul va asigura:

- utilizarea conturilor individuale de administrator;
- interzicerea conturilor administrative comune;
- jurnalizarea activităților administratorilor;
- identificarea fiecărei acțiuni administrative;
- acces administrativ doar prin conexiuni securizate.
- autentificarea administratorilor prin MPass;
- utilizarea parolelor doar în situații excepționale;

- parole complexe (minim 12 caractere);
- blocarea conturilor după încercări nereușite de autentificare;
- schimbarea periodică a parolelor, cel puțin odată la 12 luni.

14. Evidența infrastructurii și conexiunilor

Prestatorul va menține registre actualizate privind:

- adresele IP utilizate;
- IP-urile publice și interne;
- porturile și serviciile deschise;
- conexiunile externe ale sistemului;
- IP-urile utilizate de personalul tehnic pentru administrare.

15. Jurnalizare și audit

Sistemul va asigura:

- jurnalizarea activităților utilizatorilor;
- jurnalizarea autentificărilor;
- jurnalizarea operațiunilor administrative;
- păstrarea logurilor minimum 6 luni;
- protecția logurilor împotriva modificării.

16. Documentare tehnică

Prestatorul va furniza și actualiza permanent:

- arhitectura sistemului;
- diagrame tehnice;
- descrierea infrastructurii;
- manuale de utilizare;
- ghiduri de administrare;
- registrele adreselor IP și conexiunilor;
- proceduri de backup și restaurare;
- codul sursă și pachetul de instalare.

17. Raportare periodică

Prestatorul va transmite lunar:

- raport privind incidentele;
- raport SLA;
- recomandări tehnice;
- statistici privind utilizarea sistemului.

Prestatorul va transmite semestrial:

- rapoartele de sănătate ale sistemului

18. Proprietate intelectuală

Codul sursă, documentația tehnică și toate modificările realizate în cadrul contractului vor aparține beneficiarului.

19. Obligațiile părților

Prestator

- asigurarea personalului calificat;
- respectarea SLA;
- respectarea cerințelor de securitate;
- documentarea activităților.

Beneficiar

- asigurarea accesului la infrastructură;
- coordonarea tehnică;
- furnizarea informațiilor necesare.

20. Confidențialitatea informațiilor

Prestatorul este obligat să asigure confidențialitatea tuturor informațiilor la care are acces în cadrul executării prezentului contract.

Prestatorul se obligă:

- să nu divulge informațiile tehnice, operaționale sau datele prelucrate în sistem către terți fără acordul beneficiarului;
- să utilizeze informațiile accesate exclusiv în scopul executării contractului;
- să asigure că personalul implicat în prestarea serviciilor respectă obligațiile de confidențialitate;
- să implementeze măsuri adecvate de protecție a datelor și informațiilor;
- să nu copieze sau extragă date din sistem fără autorizarea beneficiarului;
- să notifice imediat beneficiarul în cazul producerii unui incident de securitate sau scurgeri de informații.

Obligațiile de confidențialitate se mențin și după încetarea contractului.

21. Transferul cunoștințelor și continuitatea administrării

Prestatorul va asigura transferul complet al cunoștințelor tehnice către Beneficiar pe durata contractului și la încetarea acestuia.

Prestatorul va asigura:

- documentarea arhitecturii sistemului și a infrastructurii tehnice;
- documentarea procedurilor de instalare, configurare și administrare;
- transmiterea tuturor manualelor și ghidurilor de administrare;

- instruirea personalului desemnat de Beneficiar privind administrarea sistemului;
- furnizarea tuturor informațiilor necesare pentru preluarea administrării sistemului de către Beneficiar sau de către un alt prestator.

La încetarea contractului, Prestatorul va acorda suport pentru transferul ordonat al administrării sistemului, fără întreruperea funcționării serviciilor.

22. Accesul Beneficiarului la infrastructură și cod

Pentru a asigura independența operațională a Beneficiarului și continuitatea serviciilor, Prestatorul va asigura:

- accesul Beneficiarului la codul sursă al sistemului;
- accesul la documentația tehnică completă;
- accesul la configurațiile infrastructurii și aplicației;
- accesul la scripturile de instalare și actualizare;
- accesul la instrumentele de monitorizare și administrare.

Beneficiarul va avea dreptul de a utiliza aceste informații pentru administrarea sistemului sau pentru transferul serviciilor către un alt prestator.

Prestatorul nu va introduce mecanisme tehnice sau contractuale care ar limita accesul Beneficiarului la sistem sau ar crea dependență exclusivă de prestator.

Calificările necesare

Prestatorul va propune o echipă dedicată implementării și mentenanței sistemului, formată din minimum 4 specialiști, prezentând CV-urile acestora. Membrii echipei trebuie să dețină cumulativ următoarele competențe, calificări și experiență profesională:

- Studii superioare în domeniul tehnologiilor informaționale sau domenii conexe;
- Cunoștințe solide în domeniul securității informaționale;
- Cunoștințe avansate în domeniul rețelisticii (Routing și Switching);
- Experiență profesională de minimum 5 ani în planificarea, proiectarea, dezvoltarea, implementarea și mentenanța sistemelor informatice;
- Experiență în administrarea și gestionarea sistemelor de aplicații;
- Experiență practică în dezvoltarea și implementarea aplicațiilor informatice;
- Experiență în dezvoltarea aplicațiilor utilizând tehnologii și limbaje de programare relevante, precum: EMC Documentum, Eroom Framework, Microsoft .NET, C++, C#, Java SE, precum și baze de date MySQL și/sau Microsoft SQL Server, demonstrată prin certificate sau alte documente justificative;
- Cunoașterea cadrului normativ național în domeniul sistemelor informaționale și comunicațiilor;
- Experiență de colaborare cu instituții publice relevante, precum Agenția Servicii Publice (ASP) și Agenția de Guvernare Electronică (e-Gov);
- Abilități dezvoltate de comunicare, analiză și sinteză, capacitate de soluționare eficientă a problemelor, lucru în echipă, adaptabilitate și inițiativă;

- Cunoașterea limbii române (scris și vorbit) la nivel avansat și cunoașterea limbii engleze la nivel tehnic.

Structura minimă a echipei propuse

Prestatorul va asigura o echipă dedicată serviciilor de mentenanță corectivă și preventivă, care va include, cel puțin, următoarele roluri:

- Coordonator de servicii (Service Manager), responsabil de gestionarea relației cu beneficiarul, monitorizarea indicatorilor de performanță (SLA) și raportarea activităților;
- Specialist suport aplicație (nivel L2/L3), responsabil de analiza și soluționarea incidentelor, precum și de acordarea suportului tehnic și funcțional;
- Dezvoltator aplicație, responsabil de remedierea defectelor (bug fixing) și realizarea ajustărilor minore necesare funcționării sistemului;
- Administrator aplicație / sistem, responsabil de configurarea, monitorizarea și menținerea funcționalității sistemului.