CAIET DE SARCINI

privind achiziționarea serviciilor de mentenanța corectivă și preventivă a sistemelor informaționale existente din cadrul Direcției Afaceri Consulare a Ministerului Afacerilor Externe și Integrării Europene.

Funcția: Companie IT, care va oferi servicii de mentenanță corectiva si preventiva a sistemelor informaționale existente din cadrul Direcției Afaceri Consulare.

Instituția: Ministerul Afacerilor Externe și Integrării Europene al Republicii Moldova.

Localitate: mun. Chișinău, Republica Moldova.

Tipul contractului: Servicii

MAEIE va contracta o Companie IT, profesioniști cu o experiență avansată în tehnologiile informaționale, pentru a oferi servicii de monitorizare continuă și capacitate de reacție 24/7, inclusiv administrarea sistemelor de aplicații soft utilizate în regim real de Direcția Afaceri Consulare a MAEIE și personalul misiunile diplomatice și oficiilor consulare ale Republicii Moldova în străinătate.

I. Obligațiunile prestatorului va implica următoarele activități generale:

1. Va prelua și asigura operaționalitatea sistemelor menționate imediat după semnarea și înregistrarea contractului;
2. Va presta servicii de monitorizare și mentenanță permanentă a sistemelor;
3. Va gestiona și asigura funcționarea eficientă și continue a sistemelor;
4. Va acționa imediat și responsabil la soluționarea integrală a tuturor problemelor raportate;
5. Va restabili funcționarea sistemului în regim de urgență;
6. Va propune soluții de îmbunătățire a sistemului pentru înlăturarea erorilor produse sistematic;
7. Va gestiona și aplica actualizările curente pentru platformă, sistemul de operare, panoul de găzduire, produsele de program utilizate;
8. Va gestiona și aplica pachetele de actualizare privind securitatea cibernetică;
9. Va gestiona și deconecta serviciile de rețea care nu sunt utilizate, va utiliza paravanul de protecție (firewall) pentru fiecare sistem;
10. Va analiza periodic riscurile, pentru identificarea și ulterior eliminarea vulnerabilităților;
11. Va oferi raportul vulnerabilităților identificate și modalitatea de înlăturare a acestora;
12. Va testa minuțios modificările efectuate în prealabil în mediile de testare;
13. Va asigura cu copii de rezervă regulat, la nivel de sistem de operare, codul aplicațiilor sistemelor, a bazelor de date, și a aplicațiilor aferente sistemelor, și va asigura revenirea la starea normală de funcționare la necesitate;
14. Va utiliza un mecanism de backup funcțional, eficient și sigur;
15. Va asigura securitatea informației și transmiterea acesteia în conformitate cu drepturile de acces atribuite personalului MAEIE și MDOC;
16. Se va conforma, și va asigura un nivel avansat de securitate în procesul de administrare a sistemelor, conform HG nr. 201 din 28 martie 2017 „Cerințele minime obligatorii de securitate cibernetică" (anexa nr. 1);

SIGV-Sistemul Informațional de Gestiune a Vizelor (inclusiv componentele acestuia-eVisa)
SIA Consul–Sistemul Informațional Automatizat Consul
SI – Sisteme Informaționale

17. Va instala și utiliza registrul evenimentelor pentru sistem cu următoarele caracteristici:
    a) păstrarea datelor pentru o perioadă de cel puțin 12 luni;
    b) înregistrarea activităților utilizatorilor în sistem, cu indicarea corectă a timpului, care trebuie să coincidă efectiv cu timpul universal coordonat (UTC) al organului competent;
    c) sistemul înregistrează conținutul monitorizării planificate și analiza acesteia, în scopul de a detecta incidentele. Datele minime înregistrate sânt: numele utilizatorului, timpul și IP adresa;
    d) sistemul va fi dotat cu un mecanism de filtrare/gestionare a mesajelor de eroare generate;
    e) descrierea procesului de modificări/aprobări ale persoanelor autorizate, testărilor și rapoartelor planificate.
18. Va prezenta în termen de două luni, planul de acțiuni privind executarea sarcinilor prevăzute în contractul respectiv, cu indicarea termenilor de realizare;
19. Va asigura un punct unic de contact, activ 24 h / 7 zile pe perioada contractării, pentru reacționarea imediată la problemele grave;
20. Va asigura un sistem eficient de raportare pentru înregistrarea incidentelor (tichete), cu posibilitatea monitorizării tichetelor și a soluțiilor aplicate;
21. Va oferi rapoarte explicite de activitate lunar, care vor cuprinde (dar fără a se limita):
    - Analiza problemelor (incidentelor) și măsurile întreprinse pentru soluționarea acestora, pentru fiecare aparte, cel puțin:
        - o Numărul unic de identificare
        - o Descriere scurtă (subiectul)
        - o Descriere mai detaliată
        - o Denumirea sistemului cu care s-a produs incident (SIACONSUL sau SIGV)
        - o Denumirea părții componente în cadrul sistemului (baza de date, web server, rețeaua, problema pe nivel fizic, etc.)
        - o Dacă problema era raportată de MAEIE - numele, prenumele și funcția persoanei care a făcut solicitare. In caz contrar, de indicat, că incidentul era detectat prin monitoring
        - o Acțiuni întreprinse pentru soluționarea problemei
        - o Timp de reacție
        - o Timp total până la soluționare
22. Va participa la definitivarea cerințelor și sarcinilor noi propuse spre implementare;
23. Va acorda suport tehnic, asistență și consultanță în procesul de utilizare a sistemelor și a echipamentului de preluare a datelor biometrice;
24. Va interacționa direct și permanent cu instituțiile interdependente în funcționarea SIGV și SIA Consul (Agenția Servicii Publice, Biroul Migrație și Azil, Poliția de Frontieră, Centrul de Guvernare Electronică, etc.), precum și identificarea de comun a soluțiilor și înlăturarea problemelor apărute/identificate;
25. Va transmite către instituție prin proces verbal codul-sursă, manualele de instalare/utilizare, în concordanță cu ultima versiune de sistemelor;

Declarație de Confidențialitate

Toate datele și informațiile primite de la personalul Ministerului pentru scopul acestei sarcini trebuie tratate în mod confidențial și sunt doar pentru a fi utilizate în legătură cu executarea acestor Termeni de Referință. Conținutul de materiale în formă scrisă obținute și folosite în această misiune nu pot fi divulgate către terțe persoane, fără autorizarea prealabilă, exprimata în scris de către MAEIE.

I. Calificările necesare:

Compania IT va veni cu CV-urile a cel puțin 4 candidați, care vor face parte din echipa asignată acestui proiect, ce vor poseda următoarele capacități, calificări, și experiențe în domeniu:

SIGV-Sistemul Informațional de Gestiune a Vizelor (inclusiv componentele acestuia-eVisa)
SIA Consul–Sistemul Informațional Automatizat Consul
SI – Sisteme Informaționale

a. Licențe în Tehnologii Informaționale;
b. Cunoștințe profunde în domeniul securității informaționale;
c. Cunoștințe avansate în Routing și Switching;
d. În mediu minim cinci ani de experiență în planificarea, proiectarea, dezvoltarea, implementarea și întreținerea sistemelor informatice;
e. Experiență în gestionarea sistemelor de aplicații;
f. Experiență în dezvoltarea și implementarea sistemelor de aplicații;
g. Experiență în dezvoltarea aplicații în baza următoarelor tehnologii și limbaje de programare, prin prezentarea certificatelor sau a altor documente ce ar confirma acest fapt: EMC Documentum, Eroom Framework, Microsoft .NET, C++, C#, Java SE, mySQL/MSSQL;
h. Cunoașterea legislației în vigoare referitoare la sistemele de informații și comunicații;
i. Experiență de conlucrare cu Agenția Servicii Publice "ASP" și Agenția de de Guvernare Electronică "eGov";
j. Abilități de comunicare, capacitate de analiză și sinteză, soluționarea eficientă a problemelor, muncă eficientă în echipă, adaptabilitate și creativitate;
k. Utilizarea fluentă și coerentă a limbii române (scris și vorbit), cunoașterea limbii engleze.

Echipa propusă de către Compania IT trebuie să fie formată din:

#	**Rolul**
1	Manager de proiect
2	Arhitector de sisteme de aplicații
3	Dezvoltatori de aplicații
4	Tester
5	Suport Tehnic

Anexa nr. 1

Cerinţele minime obligatorii de securitate cibernetică aplicabile sunt:

1) drepturile, obligaţiile, restricţiile şi responsabilităţile utilizatorilor urmează a fi stabilite de către persoana responsabilă de proces şi comunicat într-o formă stabilită responsabilului de administrare a sistemului;
2) persoana care desfăşoară activităţi de administrare a sistemului utilizează conturi diferite pentru funcţii de administrare şi funcţii de utilizator;
3) fiecare cont de utilizator este asociat cu o persoană anumită. În cazul în care sistemul prevede neadmiterea utilizării acestor conturi de către alte persoane, atunci sistemul trebuie să includă mijloace tehnice speciale, care să nu admită utilizarea acestor conturi de către persoane terţe;
4) în cazul în care sistemul nu este utilizat pentru autentificarea multifactorială, adică nu este un atribut de o natură statică (de exemplu, simbolic, un mesaj de cod-text de unică folosinţă), dar este un atribut de altă natură, utilizatorii sistemului trebuie să utilizeze o parolă;
5) utilizatorul sistemului trebuie să folosească în calitate de parolă o combinaţie din numere (0-9), caractere latine (minuscule şi majuscule) şi simboluri speciale (!#%), constituită din numărul minim de caractere, stabilit prin regulamentul intern de securitate, dar nu mai puţin de 7 caractere;
6) se interzice stocarea electronică şi transportarea în formă necriptată a parolelor utilizatorilor sistemului, inclusiv a procesului de autentificare a utilizatorilor. Se admite transportarea acestora prin reţea publică necriptată doar în cazul utilizării unei parole de o singură folosinţă, cu o valabilitate de 48 de ore de la momentul transmiterii acestora;
7) sistemul trebuie să dispună de mecanisme de gestiune a parolelor, precum şi să asigure autentificarea şi identificarea utilizatorului pentru o perioadă limitată de timp;
8) nu se admite utilizarea în produsele program a parolelor implicite (de la producător);
9) datele despre activităţile în sistem (jurnalizarea) se stochează în timp real şi se păstrează pe perioada stabilită prin regulamentul intern de securitate, dar nu mai puţin de 6 luni;
10) orice activitate în sistem trebuie să poată fi identificată într-un anumit cont de utilizator sau adresă IP;
11) managementul drepturilor de utilizator trebuie să asigure ca fiecare utilizator să poată face uz doar de drepturile sale. Verificarea activităţilor în sistem se realizează periodic, la etape de timp stabilite conform regulamentului intern de securitate, dar nu mai rar de o dată la 6 luni;
12) managementul controlului accesului trebuie să fie setat ca să permită acces autorizat din reţea externă prin Internet doar cu o parolă de o singură folosinţă, inclusiv prin semnătura electronică din cadrul serviciului electronic guvernamental de autentificare şi control al accesului (MPass).
13) parolele utilizatorilor de sistem se modifică nu mai târziu de 90 de zile calendaristice, cu limitarea posibilităţii de modificare manuală a acesteia nu mai des de două ori în decursul a 24 de ore;
14) parolele se stabilesc astfel încât să nu coincidă cu nici una dintre cele cinci parole utilizate anterior;
15) contul utilizatorului se blochează imediat în cazul în care utilizatorul a folosit parola incorect de trei ori consecutiv, cu excepţia contului administratorului de sistem. Pentru aceste cazuri se stabileşte procedura de reactivare a contului utilizatorului;
16) contul de acces al administratorului, în cazul accesării de la distanţă a sistemului, inclusiv a echipamentelor care nu se află în posesia instituţiei, este asigurat doar cu autentificarea multifactorială şi utilizarea unui canal securizat de comunicaţii.

SIGV-Sistemul Informaţional de Gestiune a Vizelor (inclusiv componentele acestuia-eVisa)
SIA Consul–Sistemul Informaţional Automatizat Consul
SI – Sisteme Informaţionale