



Elaborarea Portalului WEB al Sistemului de Poștă Electronică
Guvernamentală

Clasificare de
securitate

C4 – Public

Anexa nr. 21

la Documentația standard nr. _____

din “ _____ ” _____ 20__

CAIET DE SARCINI


**destinat achiziționării serviciilor de programare, dezvoltare și
implementare a Portalului WEB al Sistemului de Poștă Electronică
Guvernamentală (SI SPEG)**

Chișinău 2021



CUPRINS

1. Contextul achiziției	3
2. Obiectul achiziției	4
3. Scopul și abordarea de dezvoltare	4
4. Livrabile așteptate	7
5. Cerințe de raportare	7
6. Termene de implementare a proiectului	7
7. Aranjamente instituționale	8
8. Cerințe de calificare	8
9. Estimarea efortului proiectului	12
10. Modul de calculare a prețului ofertei și modul de completare a Specificațiilor de preț (Anexa nr. 23 din Documentația standard pentru realizarea achizițiilor publice de bunuri și servicii)	13
Anexa 1. Cerințe funcționale	15
A1.1. Actorii SI SPEG	15
A1.2. Cazurile de utilizare ale SI SPEG	15
A1.3. Arhitectura SI SPEG	25
Anexa 2. Cerințe tehnice	28
A2.1. Cerințe față de documentația de însoțire	28
A2.2. Cerințe față de instruirea utilizatorilor	28
A2.3. Drepturi de proprietate	29
A2.4. Cerințe față de arhitectură	29
A2.5. Cerințe de integrare	30
A2.6. Cerințe de performanță	30
A2.7. Cerințe pentru interfața utilizator	31
A2.8. Cerințe de mentenanță	32
A2.9. Cerințe de securitate	33
A2.10. Cerințe de asistență și garanție	35
A2.11. Cerințe de migrare a datelor	35
A2.12. Cerințe de asigurare calitate	36
A2.13. Cerințele procesului de acceptanță a livrabilelor de proiect	37
Anexa 3. Actele legislative și normative care reglementează procesele de business și procedurile care vor fi automatizate cu ajutorul SI SPEG	38
Anexa 4. Calcularea prețului mediu (Pm)	41

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Governamentală	Clasificare de securitate
		C4 – Public

1. Contextul achiziției

Guvernul Republicii Moldova și-a propus să modifice fundamental modul în care sunt prestate serviciile publice în Republica Moldova printr-o varietate de intervenții de modernizare a procesului de prestare a serviciilor în vederea combaterii corupției, promovării culturii de grijă față de client, precum și eficientizării administrației publice a țării.


Acest lucru este efectuat prin implementarea extensivă a soluțiilor informatice de tipul G2B, G2C și G2G. Serviciul de poștă electronică al autorităților administrației publice este un serviciu fundamental care are obiectivul de a impulsiona tranziția administrației publice spre utilizarea extensivă a spațiului digital și în același timp a securiza și standardiza instrumentele de poștă electronice utilizate de toate autoritățile publice ale Republicii Moldova.

Prezentul caiet de sarcini furnizează cerințe funcționale și nefuncționale necesare implementării unei soluții informatice guvernamentale (SI SPEG) destinate punerii în producție a unui sistem de poștă electronică pentru toate autoritățile publice ale Republicii Moldova. Acest lucru este necesar întru implementarea strategiei de consolidare a resurselor TIC a Republicii Moldova, descurajarea utilizării serviciilor de poștă electronică aflate în afara țării și asigurarea unui mediu sigur și eficient de activitate în spațiul digital a angajaților din sectorul public.

Implementarea SI SPEG urmează să aducă un șir de avantaje tehnologice și organizaționale după cum urmează:

- Consolidarea serviciilor de poștă electronică utilizate de autoritățile publice ale Republicii Moldova într-un singur serviciu, administrat centralizat și configurabil la nivelul fiecărei autorități publice centrale;
- Implementarea unui standard unic de asigurare a securității informației pentru serviciul de poștă electronică aplicabil tuturor autorităților publice ale Republicii Moldova;
- Asigurarea integrării serviciului de poștă electronică utilizat de angajații autorităților publice a Republicii Moldova cu serviciile guvernamentale de platformă (MPass, MSign, MNotify, MLog, MPower);
- Asigurarea integrării serviciului de poștă electronică utilizat de angajații autorităților publice a Republicii Moldova cu aplicații client de poștă electronică instalate pe dispozitive mobile și PC-uri;
- Furnizarea unei interfețe utilizator unice pentru toți angajații sectorului public care va asigura accesul la funcționalități specifice tendințelor moderne ale serviciilor de poștă electronică: gestiune mesaje email, partajare fișiere, planificare și gestiune evenimente de calendar, gestiune notițe, conversații confidențiale etc.
- Asigurarea unei configurabilități la nivel de serviciu per ansamblu, autoritate publică și cont particular al utilizatorului de poștă electronică.

Proiectarea, dezvoltarea și implementare SI SPEG vine să îndeplinească prevederile Hotărârii Guvernului nr. 822 din 06.11.2012 cu privire la serviciile sistemului de poștă electronică al autorităților administrației publice, Hotărârii Guvernului nr. 414 din 08.05.2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat și Hotărârii Guvernului nr. 201 din 28.03.2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică, urmând să furnizeze un impact benefic în activitatea autorităților publice a Republicii Moldova.

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Governamentală	Clasificare de securitate
		C4 – Public

2. Obiectul achiziției

Serviciul Tehnologia Informației și Securitate Cibernetică este interesată în identificarea unei companii prestatoare de servicii informatice capabile să propună o echipă capabilă și experimentată să dezvolte Portalul Web al Sistemului de Posta Electronica Governamentală (SI SPEG) în baza metodologiei Agile.

SI SPEG urmează a fi implementat de o echipă competitivă de specialiști care corespund cerințelor specificate în capitolul 8 al prezentului caiet de sarcini. Specialiștii propus de ofertanți trebuie să fie disponibili full-time pe parcursul activităților de proiect (în funcție de faza proiectului specialiștii alocați activităților specifice fazei trebuie să lucreze exclusiv pentru SI SPEG și să nu fie alocați în paralel în cadrul altor proiecte ale companiei dezvoltatoare) astfel ca activitățile din planul de implementare să deruleze fără întreruperi.

Efortul necesar al lucrărilor de proiectare, dezvoltare și implementare a SI SPEG este estimat la **1170 om/zile (sau 9360 om/ore) și exercitat de 9 experți cheie** conform estimărilor stipulate în Tabelul 1 din capitolul 9 al prezentului caiet de sarcini. Perioada de implementare o constituie **8 luni** calendaristice pe parcursul căreia compania dezvoltatoare va asigura disponibilitatea și implicarea experților solicitați.

Estimările stipulate în Tabelul 1 din capitolul 9 sunt preventive, astfel încât în funcție de evoluția proiectului efortul planificat unor categorii de experți **poate fi alocat altora dar nu va depăși cuantumul total de 1170 om/zile (sau 9360 om/ore).**

3. Scopul și abordarea de dezvoltare

Scopul achiziției constă în proiectarea, dezvoltarea, configurarea și implementarea SI SPEG în conformitate cu cerințele funcționale și nefuncționale identificate definite iterativ de către STISC (setul preventiv de cerințe este prezentat în anexele 1 și 2 și urmând abordarea de dezvoltare descrisă mai jos.

Dezvoltarea soluției se va face după principiul de dezvoltare iterativă și agilă. Deoarece există mai multe metodologii de dezvoltare agilă a produselor software și pentru a evita neînțelegerile, această secțiune oferă principii cheie care trebuie respectate în procesul de proiectare, dezvoltare și implementare a soluției informatice.

3.1. Dezvoltare iterativă

Spre deosebire de abordarea de dezvoltare cascadă, soluția va fi dezvoltată în iterații numite sprinturi. Aceasta înseamnă că implementarea funcționalităților sistemului se va face în etape, unele module fiind în producție, în timp ce altele sunt încă în curs de dezvoltare. Prioritizarea sarcinilor care urmează a fi incluse într-o iterație va fi stabilită de Beneficiar. Durata iterației va fi stabilită de STISC împreună cu Furnizorul soluției software.

3.2. Dezvoltare Agile

În procesul de dezvoltare se vor aplica principiile Agile pentru a permite operarea modificărilor și flexibilitate în implementare. STISC va furniza lista cerințelor generice din care urmează să fie detaliat backlog-ul soluției. Furnizorul va efectua analiza de business necesară și va aproba împreună cu STISC backlog-ul soluției. Backlog-ul va include cerințe de operare și tehnice ordonate în modul în care STISC consideră necesar.

Articolele în backlog-ul produsului sunt ordonate de către STISC după prioritate. STISC este liber să-și gestioneze backlog-ul, adăugând, eliminând sau schimbând ordinea articolelor din acesta la dorință. La începutul fiecărui sprint, se selectează cele mai importante articole care se încadrează într-un sprint și din ele se creează un sprint backlog.

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Governamentală	Clasificare de securitate
		C4 – Public

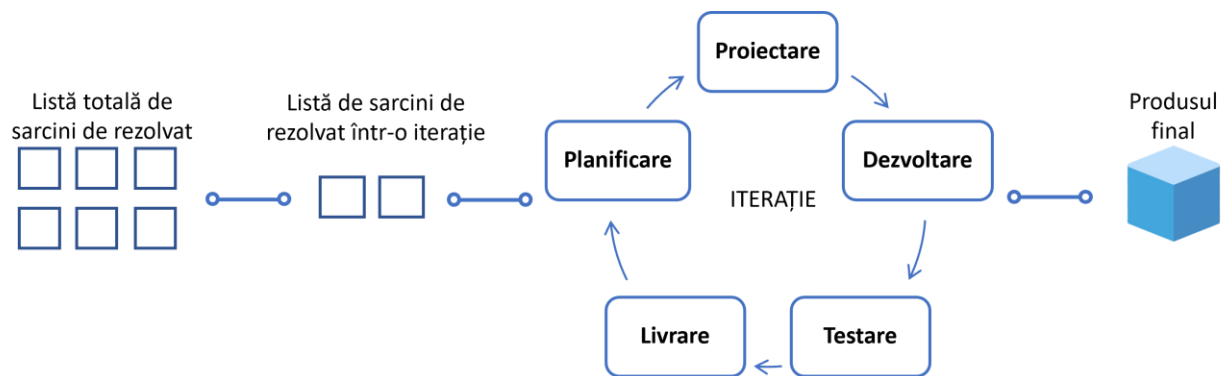


Figura 1. Descrierea indicativă a ciclului/procesului de dezvoltare Agile.

Articolele din acest sprint backlog sunt în continuare detaliate de către Furnizor, coordonate cu STISC pentru a aproba modelul de implementare și distribuite dezvoltatorilor pentru realizare. Sprint backlog-ul nu se modifică în procesul de derulare a sprintului.

3.3. Produs funcțional la fiecare iterație

Fiecare sprint finalizează cu un produs funcțional, care este prezentat către STISC pentru acceptare în ultima (ultimele) zi (zile) ale sprintului. Produsul funcțional va îndeplini criteriile convenite – Definiția lui „Finalizat” – produsul livrat trebuie să fie pe deplin funcțional și testat, însoțit de teste unitare relevante, însoțit de documentația relevantă dacă este cazul, codul sursă complet furnizat etc.


Plățile vor fi efectuate trimestrial în cazul livrării cu succes a pachetelor de lucru (unul sau mai multe livrabile conform planului de lucru agreat în comun). În cazul în care livrabilele conțin defecte din motive neimputabile STISC, Furnizorul le va înlătura fără careva modificări de grafic sau costuri, inclusiv posibile vizite la Client.

Produsele funcționale rezultate din diferite sprinturi pot fi combinate la discreția STISC într-o versiune lansată în producție. Orice incident raportat de Beneficiar după lansare va fi soluționat de Furnizor în conformitate cu Acordurile privind nivelul serviciilor (ANS) definite în Anexa 2, punctul A2.10 Asistență și garanție.

Pentru a asigura livrarea la timp a produselor de către echipa de dezvoltatori, un reprezentant al STISC, numit de regulă „Proprietarul produsului” (Product owner) în metodologiile Agile, va fi permanent la dispoziția echipei pentru a răspunde la întrebările echipei, astfel evitând încetinirea procesului de implementare.

Furnizorul va avea în echipa de proiect o persoană cu rol de „Business analyst” care va îndeplini totalitatea lucrărilor de analiză, proiectare de detaliu și coordonare a soluției de implementare cu STISC. Business analistul va fi responsabil de elaborarea în inițială a backlog-ului SI SPEG, coordonarea acestuia cu Proprietarul produsului pentru a stabili prioritățile de dezvoltare. Furnizorul împreună cu STISC va actualiza cu regularitate backlog-ul produsului pentru a reflecta lista prioritizată a funcționalităților dorite a fi implementate.

Business analistul împreună cu echipa de dezvoltare va analiza domeniul și va propune soluții optime de implementare. STISC va asigura înțelegerea corectă a cerințelor față de soluție și va ghida Furnizorul în procesul de proiectare și implementare a sistemului informatic.

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Governamentală	Clasificare de securitate
		C4 – Public

3.4. Implicarea STISC

Spre deosebire de modelul waterfall (cascadă) utilizat frecvent la achiziția și implementarea sistemelor informatice guvernamentale, persoana desemnată de STISC – Proprietarul produsului – va fi implicată intens în procesul de dezvoltare. Proprietarul produsului va avea trei responsabilități importante:

1. Va menține backlog-ul produsului. Proprietarul produsului împreună cu Business Analistul va actualiza cu regularitate backlog-ul produsului pentru a reflecta lista prioritizată a funcționalităților dorite a fi implementate.
2. Va răspunde la întrebările dezvoltatorilor. Proprietarul produsului va fi permanent disponibil pentru a răspunde la întrebările de clarificare ale echipei de dezvoltatori, astfel evitând comunicarea complexă și formală în cadrul proiectului. Pentru a obține un produs funcțional la sfârșitul sprintului, este extrem de important ca echipa să dispună de toate informațiile necesare la momentul oportun.
3. Va accepta pachetele de lucru. Pachetele de lucru livrate sunt prezentate Clientului la sfârșitul fiecărui sprint pentru acceptare. Clientul va accepta pachetul de lucru sau va informa pe Furnizor despre defectele identificate până la finalizarea următorului sprint.

Deși nu este strict necesar, Proprietarul produsului poate participa la ședințele echipei de dezvoltare pentru a se informa despre progresele înregistrate și eventualii factori blocați pentru o reacție promptă la aceștia.

Proprietarul produsului, de asemenea, ia decizia privind lansarea produsului în conformitate cu planul de lansare.

În conformitate cu principiile metodologiei Agile de management al proiectului, STISC va trasa viziunea de dezvoltare a produsului precum și Foaia de parcurs a acestuia pentru a monitoriza progresul și pentru a asigura dezvoltarea corespunzătoare a produsului.

3.5. Garanție


Soluția dezvoltată va avea o garanție de 12 luni. Perioada de garanție începe după lansarea finală în producție a SI SPEG. În timpul perioadei de garanție Furnizorul va elimina toate defectele identificate.

Dezvoltarea și exploatarea trebuie să fie în conformitate cu documentele legislative și normative enumerate în Anexa 3.

3.6. Stiva tehnologică

Pentru o mai bună valorificare a investițiilor în e-Guvernare, soluția va fi dezvoltată utilizând ultimele versiuni ale următoarelor stive tehnologice:

- Limbaj de programare: C#
- *Soluție ORM*: Entity Framework Core.
- *Cadrul web*: ASP.NET MVC Core.
- *SGBD*: Microsoft SQL Server.
- Server de poștă: Zimbra.
- Motor al containerului: Docker.
- Orchestrator containere: Kubernetes.
- Server de memorie cache și session store: Microsoft SQL Server sau Redis.

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Governamentală	Clasificare de securitate
		C4 – Public

În procesul de dezvoltare a SI SPEG Furnizorul sau STISC pot propune utilizarea unor componente adiționale necesare pentru dezvoltarea și funcționalitatea adecvată a soluției în producție.

4. Livrabile așteptate

În cadrul activităților necesare îndeplinirii obiectivelor stipulate în prezentul caiet de sarcini Furnizorul va furniza următoarele livrabile:

1. **Un concept al SI SPEG.** Furnizorul va elabora un concept de nivel înalt (HLD) al viitoarei soluții informatice care să cuprindă aspectele principale de implementare (obiectivele de implementare, arhitectura, stiva tehnologică, infrastructura de desfășurare, componentele funcționale, mock-up-uri ale interfețelor principale, Planul de implementare a proiectului cu estimarea efortului necesar pentru fiecare "Caz de utilizare (CU)" (Use Case), etc.). În baza Conceptului aprobat de STISC vor fi demarate iterațiile de dezvoltare și implementare a SI SPEG.
2. **Un sistem informatic (SI SPEG) pe deplin funcțional** Furnizorul va livra un cod sursă compilabil și documentat (inclusiv biblioteci și instrumente terțe, licențe, dacă este cazul, și scenarii de automatizare).
3. **Documentația tehnică și documentația utilizatorului final** elaborată în conformitate cu cerințele STISC cuprinse în Anexa 2.
4. **Sesiuni și materiale de instruire** elaborate în conformitate cu cerințele STISC expuse în Anexa 2.


5. Cerințe de raportare

În cadrul activității vor fi prezentate următoarele rapoarte:

- a) Raportul Sprint, inclusiv comunicatele de lansare, dezagregarea și durata sarcinilor implementate în timpul sprintului, durata, aspectele și problemele majore, propuneri de acțiuni ulterioare;
- b) Următorul Sprint Backlog, inclusiv dezagregarea și durata estimată a sarcinilor propuse pentru implementare la următorul sprint, resursele pe care Furnizorul le așteaptă de la STISC și/sau acțiunile care urmează a fi întreprinse de Client;
- c) Rapoarte de instruire, prezentate după fiecare sesiune de instruire, inclusiv:
 - Lista participanților;
 - Agenda sesiunii de instruire;
 - Materialele de instruire (prezentări, laboratoare etc.);
 - Rezultatele evaluării participanților.

6. Termene de implementare a proiectului

Sarcinile enumerate în prezentul document sunt estimate a fi îndeplinite în 20 de luni: 8 luni pentru proiectare/dezvoltare/migrare/implementare și 12 luni de garanție, mentenanță și suport tehnic. Deși, scopul principal al perioadei de garanție este identificarea și remedierea erorilor, dacă STISC va identifica în perioada de garanție funcționalități noi necesare de a fi implementate, acestea pot fi implementate în iterații suplimentare, în funcție de bugetul disponibil.

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Governamentală	Clasificare de securitate
		C4 – Public

7. Aranjamente instituționale

STISC este responsabil de toate aspectele administrative și procedurale, managementul contractului și financiar, inclusiv acceptarea și efectuarea plății pentru livrabile/rapoartele prevăzute de Contract, responsabilitățile generale ce țin de proiect și coordonarea eficientă cu factorii interesați.

STISC va desemna Proprietarul produsului (Product owner /Manager de produs), care va coordona și lua decizii privind toate aspectele ce țin de elementele tehnice ale Contractului. Proprietarul produsului va decide asupra dății lansării procesului de implementare a contractului și alte atribuții.

STISC va asigura următoarele:

- resursele de infrastructură pentru mediul de testare și producție;
- repozitoriul pentru codul sursă, sistemul de identificare și gestiune a problemelor, mediul de integrare și livrare continuă (CI/CD), sistemul de gestiune a sarcinilor.
- facilitățile de instruire.

Furnizorul va asigura condiții de lucru (spațiu de lucru/oficii pentru experți, echipament de oficiu, calculatoare, rețele de comunicare etc.) și servicii adecvate pentru personalul Furnizorului pe perioada proiectului.

Furnizorul va fi responsabil pentru managementul zilnic al echipei de proiect și disponibilitatea tuturor resurselor necesare.

Furnizorul va organiza ședința de lansare a activității (Kick-off meeting) și discuția inițială Backlog la sediul STISC. La aceste sesiuni vor participa toți experții cheie ai Furnizorului, în conformitate cu secțiunea privind Cerințele de calificare. Costurile legate de prezența STISC la ședința de lansare vor fi acoperite de Furnizor și nu vor fi incluse în propunerea financiară a Furnizorului.

Furnizorul va întreprinde vizite la STISC pentru a instrui utilizatorii finali.

În cazul în care livrabilele conțin defecte și/sau sunt întârzieri din motive neimputabile Furnizorului care pot afecta rezultatele proiectului, Furnizorul i se poate solicita să întreprindă vizite la STISC pentru a soluționa problemele apărute.

Limba de perfectare a livrabilelor de proiect și de comunicare în cadrul activităților de proiect va fi româna.


În activitatea sa Furnizorul va fi supravegheat de Proprietarul produsului, raportând conducerii al STISC.

8. Cerințe de calificare

8.1. Cerințele de calificare față de compania dezvoltatoare

Furnizorul va prezenta documente justificative (inclusiv informații despre contractele finalizate și informațiile de contact ale clienților de la care pot fi solicitate referințe sau pe care STISC ar putea, la necesitate, vizita pentru a se familiariza cu sistemele puse în exploatare de Furnizor) pentru a se convinge că cel din urmă satisface cerințele de mai jos cu privire la experiență:

1. A fost operațional în ultimii 5 ani, cea mai mare parte a activității ținând de dezvoltarea sistemelor informatice.
2. Deține experiență de implementare a proiectelor similare în amploare și complexitate dezvoltând aplicații web utilizând tehnologiile .NET, demonstrată prin cel puțin 2 contracte cu etapa de dezvoltare finalizată în cel puțin 3 ani. Pentru proiectele în derulare, vor fi prezentate copii ale documentelor de acceptare a întregii soluții software.

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Guvernamentală	Clasificare de securitate
		C4 – Public

3. Experiența de dezvoltare software cu utilizarea principiilor Agile (în conformitate cu descrierea din secțiunea privind domeniul de intervenție și abordare din Caietul de Sarcini) va fi un avantaj. Acest lucru va fi demonstrat prin prezentarea metodologiei proiectului care va descrie rolul Furnizorului.
4. Experiență demonstrată de utilizare a stivei tehnologice și deținerea certificatelor aferente stivei tehnologice, proceselor de asigurare calitate și securității informației va fi un avantaj.

8.2. Cerințe minime de calificare față de personalul Furnizorului

Furnizorul va propune o echipă formată din următorii experți cheie:

- Expert cheie 1 (1 persoana): Business analyst/Team Leader/Scrum master;
- Expert cheie 2 (2 persoane): Dezvoltator software interfață FrontEnd;
- Expert cheie 3 (2 persoane): Dezvoltator software interfață BackEnd;
- Expert cheie 4 (1 persoana): Dezvoltator software/ Specialist DevOps
- Expert cheie 5 (1 persoana). Dezvoltator/Administrator bază de date;
- Expert cheie 6 (1 persoana). Software Tester și Formator;
- Expert cheie 7 (1 persoana). Designer


Pentru experții cheie propuși, vor fi prezentate CV-urile care demonstrează îndeplinirea cerințelor minime de calificare, după cum urmează:

Expert cheie 1. Business analyst/Team Leader/Scrum master

Business analistul este responsabil de realizarea legăturii de zi cu zi cu Clientul și urmează să asigure coordonarea internă și ghidarea tuturor experților proiectului, precum și coordonarea cu partenerii externi. Acest expert va asigura, de asemenea, disponibilitatea experților necesari în conformitate cu Planul de activitate al Proiectului și va supraveghea îndeplinirea obligațiilor de raportare în timp util și la un nivel înalt de calitate. Expertul cu rol de Business Analist trebuie să corespundă următoarelor cerințe de calificare:

- studii superioare în domeniul TIC sau alt domeniu relevant;
- cel puțin 7 ani de experiență în dezvoltarea software;
- cel puțin 5 ani de experiență demonstrată în analiză de business, managementul echipei/proiectului cu aplicarea metodologiei Agile, cu cel puțin 2 proiecte implementate în ultimii 3 ani;
- cel puțin 3 ani de experiență în dezvoltarea software cu utilizarea C#, Entity Framework, ASP.NET MVC, Microsoft SQL Server și a unui cadru de injectare a dependențelor (dependency injection framework);
- deținerea certificărilor în orice tehnologie din stiva tehnologică solicitată se va considera un avantaj și procesele de management ale proiectelor;
- experiență în testarea unitară, integrarea continuă, DevOps;
- experiență în analiza sistemelor;
- abilitate de comunicare în limba română.

Expert cheie 2. Dezvoltator interfață FrontEnd


	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Governamentală	Clasificare de securitate
		C4 – Public

- Această categorii de dezvoltatori este responsabilă de dezvoltarea interfeței utilizator accesibilă beneficiarilor de poștă electronică (interfața de accesare a serviciilor furnizate de SI SPEG către utilizatorii cu rol Utilizator SPEG) și trebuie să corespundă următoarelor cerințe de calificare: studii superioare în domeniul TIC sau alt domeniu relevant;
- cel puțin 5 ani de experiență în dezvoltarea software;
- cel puțin 5 ani de experiență demonstrată în dezvoltarea aplicațiilor WEB;
- cel puțin 3 ani de experiență în dezvoltarea software cu utilizarea C#, Entity Framework, ASP.NET MVC și Microsoft SQL Server;
- experiență demonstrată în proiectarea și dezvoltarea interfețelor WEB utilizator cu utilizarea cadrelor responsive, aplicațiilor web progresive;
- participarea în cel puțin 2 proiecte de dezvoltare software în ultimii 3 ani cu aplicarea metodologiei Agile;
- experiență în testarea unitară;
- deținerea certificărilor în orice tehnologie din stiva tehnologică solicitată se va considera un avantaj;
- abilitate de comunicare în limba română.

Expert cheie 3. Dezvoltator interfață BackEnd

Categorie de dezvoltatori responsabilă de dezvoltarea componentei BackEnd a SI SPEG accesibilă utilizatorilor cu rol de Administrator pentru exercitarea atribuțiilor de configurare, monitorizare și administrare a SI SPEG. Dezvoltatorul BackEnd trebuie să corespundă următoarelor cerințe de calificare:

- studii superioare în domeniul TIC sau alt domeniu relevant;
- cel puțin 5 ani de experiență în dezvoltarea software;
- cel puțin 5 ani de experiență demonstrată în dezvoltarea aplicațiilor WEB;
- cel puțin 3 ani de experiență în dezvoltarea software cu utilizarea C#, Entity Framework, ASP.NET MVC și Microsoft SQL Server;
- experiență demonstrată în proiectarea și dezvoltarea interfețelor WEB utilizator cu utilizarea cadrelor responsive, aplicațiilor web progresive;
- participarea în cel puțin 2 proiecte de dezvoltare software în ultimii 3 ani cu aplicarea metodologiei Agile;
- experiență în testarea unitară;
- deținerea certificărilor în orice tehnologie din stiva tehnologică solicitată se va considera un avantaj;
- abilitate de comunicare în limba română.

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Guvernamentală	Clasificare de securitate
		C4 – Public

Expert cheie 4. Dezvoltator software/ Specialist DevOps

Categorie cheie de dezvoltator responsabil de implementarea mecanismelor DevOps în procesul de dezvoltare și implementare a SI SPGE și implicarea în procesele de dezvoltare critice. Această categorie de experți trebuie să corespundă următoarelor cerințe de calificare:

- studii superioare în domeniul TIC sau alt domeniu relevant;
- cel puțin 5 ani de experiență în dezvoltarea software;
- experiență în dezvoltarea software cu utilizarea C#, Entity Framework, ASP.NET MVC, Microsoft SQL Server;
- participarea în cel puțin 2 proiecte de dezvoltare software în ultimii 3 ani cu aplicarea metodologiei Agile;
- experiență demonstrată de testare unitară, integrare continuă, DevOps;
- deținerea certificărilor în orice tehnologie din stiva tehnologică solicitată se va considera un avantaj;
- abilitate de a comunica în limba română.


Expert cheie 5. Dezvoltator/Administrator bază de date

Categorie de dezvoltator responsabilă de proiectarea și administrarea bazei de date aferente SI SPEG. În virtutea funcției deținute, categoria dată de experți urmează să definească structurile de date aferente SPEG, să implementeze procedurile stocate ale bazei de date a SI SPEG, să configureze drepturile și privilegiile la nivel de bază de date pentru toate categoriile de utilizatori SI SPEG, să implementeze mecanismul de backup al bazei de date, să implementeze mecanismul de migrare a datelor și populare inițială a bazei de date SI SPEG. Dezvoltatorul/Administratorul bazei de date trebuie să corespundă următoarelor cerințe de calificare:

- studii superioare în domeniul TIC sau alt domeniu relevant;
- cel puțin 5 ani de experiență în dezvoltarea software;
- cel puțin 3 de experiență în dezvoltarea software cu utilizarea C#, Entity Framework, Microsoft SQL Server;
- participarea în cel puțin 2 proiecte implementate în ultimii 3 ani cu aplicarea metodologiei Agile;
- experiență de testare unitară (engl. unit testing);
- deținerea certificării în orice tehnologie din stiva tehnologică solicitată va fi un avantaj;
- experiență demonstrată în proiectarea, dezvoltarea și optimizarea bazelor de date;
- abilitate de a comunica în limba română.

Expert cheie 6. Software Tester și Formator

Categorie de dezvoltator responsabilă de asigurarea calității proceselor de dezvoltare și implementare a SI SPGE (testarea funcțională și nefuncțională a SI SPEG inclusiv prin intermediul mijloacelor automatizate), elaborarea documentației de utilizare a SI SPEG și

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Guvernamentală	Clasificare de securitate
		C4 – Public

efectuarea instruirilor pentru categoriile de utilizatori menționați în prezentul caiet de sarcini. Acest tip de expert trebuie să corespundă următoarelor cerințe de calificare:

- studii superioare în domeniul TIC sau alt domeniu relevant;
- cel puțin 3 ani de experiență în testarea software în proiecte de complexitate similară;
- experiență demonstrată în analiza testării și proiectare software;
- experiență demonstrată în testarea de performanță (load and stress) și testarea de securitate;
- experiență demonstrată în testarea automată;
- deținerea certificării în orice tehnologie din stiva tehnologică solicitată va fi un avantaj;
- experiență în realizarea sesiunilor de instruire pentru utilizatori finali și specialiști IT;
- experiență de scriere a documentației tehnice și documentației destinate pentru utilizatorul final;
- abilitate de a comunica în limba română.

Expert cheie 7. Designer

Designerul este responsabil de proiectarea și implementarea aspectului interfeței utilizator a SI SPEG, propunerea soluțiilor de sporire a ergonomiei și accesibilității interfeței utilizator pentru toate categoriile de utilizatori, asigurarea implementării prevederilor legislației în vigoare standardele și bunele practici internaționale în domeniu.

Designerul trebuie să corespundă următoarelor cerințe de calificare:

- studii superioare în domeniul TIC sau alt domeniu relevant;
- cel puțin 3 ani de experiență în proiectarea și machetarea interfețelor utilizator în proiecte de complexitate similară;
- experiență demonstrată în analiza cerințelor față de interfața utilizator;
- experiență demonstrată în testarea interfețelor utilizator și analiza comportamentală a utilizatorilor;
- participarea în cel puțin 2 proiecte implementate în ultimii 3 ani cu aplicarea metodologiei Agile;
- deținerea certificării în orice tehnologie din stiva tehnologică solicitată va fi un avantaj;
- abilitate de a comunica în limba română.

9. Estimarea efortului proiectului

Tabelul 1 conține o evaluare prealabilă a efortului necesar proiectării, dezvoltării și implementării SI SPEG pentru toate categoriile de experți solicitate în capitolul 8 al prezentului caiet de sarcini.

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Governamentală	Clasificare de securitate
		C4 – Public

Tabelul 1. Estimarea efortului destinat implementării SI SPEG

#	Denumirea categoriei expertului	Om/ore	Cantitatea persoanelor	Total om/ore
1.	Business analist/ Team Leader/ Scrum master	1120	1	1120
2.	Dezvoltator software interfață FrontEnd	1360	2	2720
3.	Dezvoltator software interfață BackEnd	1360	2	2720
4.	Dezvoltator software/ Specialist DevOps	480	1	480
5.	Dezvoltator/ Administrator bază de date	560	1	560
6.	Software Tester și Formator	1120	1	1120
7.	Designer	640	1	640
TOTAL		-	9	9360

Experții din echipa de dezvoltare vor activa în limita efortului inclus în tabelul 1. Considerând metodologia Agile de dezvoltare, la necesitate, STISC poate realoca volumul de lucru rezervat experților implicați în proiectul de dezvoltare SI SPEG, astfel încât efortul care nu a fost folosit de către unii experți să poată fi distribuit către alții.

Plata se va efectua în baza Facturilor fiscale emise de către Furnizor, suma fiind calculată reieșind din efortul efectiv depus de către experții Furnizorului, agreat în comun cu STISC, în baza actelor de acceptare a SPRINT-urilor de proiect. În actele de acceptanță se va indica Sprint-ul, volumul efortului în om/ore depus de către fiecare categorie de experți. Suma spre facturare și plată se va calcula din volumul efortului indicat în Actul de acceptanță la prețurile indicate de către ofertant pentru fiecare categorie de expert în coloana 7 "Prețul ofertantului pentru 1 om/oră, fără TVA, MDL" din formularul *Calcularea prețului mediu* din Anexa 4.


10. Modul de calculare a prețului ofertei și modul de completare a Specificațiilor de preț (Anexa nr. 23 din Documentația standard pentru realizarea achizițiilor publice de bunuri și servicii)

10.1 Preț mediu

Ofertantul urmează să completeze și să prezinte în oferta sa, ca fișier separat, semnat electronic, formularul "Calcularea prețului mediu" din Anexa 4. Prețul unitar reprezintă o medie de preț pentru 1 om/oră, în dependență de ponderea volumului de efort estimat pentru fiecare categorie de expert, din totalul efortului estimat în Tabelul 1. În acest formular, la coloana 7 "Prețul ofertantului pentru 1 om/oră, fără TVA, MDL" ofertantul urmează să indice prețul pentru 1 om/oră pentru fiecare categorie de expert. La coloana 8 "Preț mediu, MDL" se va indica rezultatul înmulțirii coloanei 6 cu coloana 7 (Pondere, % * Prețul ofertantului pentru 1 om/oră, MDL).


10.2. Prețul ofertei

Ofertantul urmează să completeze, să semneze și să prezinte în oferta sa, Specificațiile de preț (Anexa nr. 23 din Documentația standard publicată de către Autoritatea contractată în SIA RSAP la procedura

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Governamentală	Clasificare de securitate
		C4 – Public

respectivă). La Specificații de preț (Anexa nr. 23 din Documentația standard pentru realizarea achizițiilor publice de bunuri și servicii) în coloana 4 "Cantitate", se va indica volumul maxim total de efort din Tabelul 1, ce constituie – 9360 om/ore. La coloana 5 "Preț unitar (fără TVA)" **se va indica Suma (Pm) din formularul "Calcularea prețului mediu (Pm)" din Anexa nr. 4.**

Suma cu TVA indicată în formularul Specificații de preț (Anexa nr. 23 din Documentația standard pentru realizarea achizițiilor publice de bunuri și servicii) va constitui suma maximală a Contractului și nu poate fi depășită.

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Guvernamentală	Clasificare de securitate
		C4 – Public

Anexa 1. Cerințe funcționale

Această anexă descrie cerințele funcționale ale SI SPEG. Cerințele funcționale identifică ce face sistemul informatic. De asemenea, sunt definite funcțiile specifice (actorii) care stabilesc ce funcționalități trebuie să furnizeze SI SPEG.

Cerințele funcționale sunt definite folosind „Cazuri de utilizare”. Fiecare caz de utilizare este descris ca un set de funcții prin care va acționa utilizatorul.

A1.1. Actorii SI SPEG

Următorii actori vor fi implicați în gestiunea SI SPEG și vor acționa cu diferite capacități:

Administrator SPEG – categorie de utilizatori cu rol de administrare tehnică a SI SPEG, care acționează în numele STISC. Deși sarcinile de administrare în cadrul SI SPEG ar putea fi îndeplinite de alte roluri (stabilite ulterior), în contextul prezentului document „Administratorul SPEG” va cumula toate sarcinile de administrare tehnică a SI SPEG.

Administrator delegat SPEG – categorie de utilizatori care îndeplinește sarcini de administrare tehnică în limita drepturilor care i-au fost delegate de Administratorul SPEG. Atribuțiile sale pot fi limitate atât la nivel de funcționalități, cât și la nivel instituțional (exemplu: administrarea spațiului SPEG rezervat unei autorități publice sau a unei subdiviziuni a acesteia).

Utilizator SPEG – categorie de utilizatori cu drept de utilizare a serviciului de poștă electronică guvernamentală. Un utilizator SPEG este identificat cu persoana care este angajată în domeniul serviciului public și i-a fost creat un cont de poștă electronică guvernamentală. Utilizatorul SPEG are acces la totalitatea funcționalităților SPEG destinate exploatării serviciului de poștă electronică guvernamentală și serviciilor aferente acesteia, furnizate de SI SPEG.

A1.2. Cazurile de utilizare ale SI SPEG

Diagrama din figura 2 descrie principalele cazuri de utilizare ale SI SPEG, prin care acest sistem informațional va furniza totalitatea funcționalităților necesare actorilor sistemului. Fiecare caz de utilizare de nivel superior, corespunde unui „Epic” al metodologiei Agile, care urmează a fi descompus în mai multe „User Stories” (în funcție de specificul cazului de utilizare).

CU01: Gestionez mesaje

Reprezintă un caz de utilizare complex care furnizează funcționalitățile de bază specifice unui serviciu de poștă electronică (inclusiv facilități de navigare și explorare a mesajelor Email, organizarea acestora și aplicarea etichetelor în funcție de preferințele utilizatorului SI SPEG).

Utilizatorul SI SPEG va gestiona cel puțin următoarele categorii de mesaje Email:


- **Mesaje de intrare** – totalitatea mesajelor recepționate de Utilizatorul SI SPEG prin intermediul serviciului de poștă electronică furnizat de SI SPEG;
- **Mesaje de ieșire** – totalitatea mesajelor Email expediate de Utilizatorul SI SPEG prin intermediul serviciului de poștă electronică furnizat de SI SPEG;
- **Mesaje nefinalizate** – totalitatea mesajelor Email care se află în statut de ciornă în cadrul SI SPEG și încă nu au fost expediate destinatarilor;
- **Mesaje programate** – totalitatea mesajelor Email pentru care Utilizatorul SI SPEG a setat un moment în timp când SI SPEG urmează a le expedia automat destinatarilor.



Figura 2. Diagrama cazurilor de utilizare ale SI SPEG

Mecanismul de gestiune a mesajelor Email presupune existența următoarelor facilități furnizate de SI SPEG:

- **CU01.1: Primesc/expediez mesaje email.** Funcționalitate de recepționare și expediere a mesajelor Email. Utilizatorul SI SPEG va dispune de toate instrumentele necesare pentru redactarea unui mesaj E-mail. Astfel, un editor de tip WYSIWYG trebuie să fie utilizat pentru redactarea textului cu balize HTML minim necesare pentru formatarea textului, aplicarea stilurilor, elaborarea tabelor, inserarea imaginilor și hyperlink-urilor, etc. Totodată, trebuie să existe posibilitatea redactării mesajului Email într-un format capabil pentru a fi semnat electronic.

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Guvernamentală	Clasificare de securitate
		C4 – Public

După acționarea butonului de expediere a mesajului, SI SPEG va amâna expedierea cu un interval predefinit de timp în decursul căruia utilizatorul poate renunța la expedierea mesajului Email.


Utilizatorul SI SPEG va dispune de funcționalitate de expediere a mesajelor Email unei liste extinse de destinatari. Înainte de expediere, Utilizatorul SI SPEG va putea selecta una din opțiunile de expediere:

- a) Expediere mesaj Email împreună cu partajarea listei de destinatari (opțiune implicită). În așa mod, receptorii mesajului Email vor putea vedea toți destinatarii mesajului Email. Această opțiune presupune o listă limitată de destinatari. Limita numărului maxim de destinatari va fi configurată de către Administratorul SI SPEG.
- b) Expediere mesaj Email pentru fiecare destinatar în parte. Astfel, chiar dacă mesajul conține o listă de destinatari, respectivii vor recepționa mesajul în mod individual, fără a putea vedea ceilalți destinatari ai acestui mesaj. Aici, la fel, lista de destinatari poate fi limitată, iar această limită este configurată de către Administratorul SI SPEG.

Înainte de expedierea mesajului, Utilizatorul SI SPEG poate marca conversația ca fiind confidențială. Pentru mesajele Email confidențiale vor fi dezactivate opțiunile de redirectionare către alți destinatari care nu fac parte din lista inițială a acestora. Mesajele Email care au fost marcate ca fiind confidențiale vor fi expediate cu un antet textual în care este expusă clauza de confidențialitate. Fișierele partajate prin intermediul acestor mesaje vor fi implicit disponibile pentru vizualizare și descărcare doar destinatarilor acestor mesaje.

- **CU01.2: Programez expediere mesaj.** Funcționalitate disponibilă Utilizatorului SPEG prin intermediul căreia acesta va avea posibilitatea de a planifica expedierea mesajului Email pentru un anumit moment de timp (dată, oră și minut). Utilizatorul SI SPEG va putea defini explicit momentul planificat al expedierii (*exemplu: prin alegerea dintr-un calendar a valorii relevante*) sau alege valori predefinite (*exemplu: „Mâine la ora 8:00”*). Odată programată expedierea, mesajul Email va trece în lista mesajelor programate pentru expediere. Utilizatorul SI SPEG va avea acces la funcționalități de anulare sau redactare a mesajelor din lista de așteptare a fi expediate programat. Mesajele pentru care a fost anulată expedierea vor trece în lista mesajelor nefinalizate în statut de ciornă.
- **CU01.3: Clasific mesaje, aplic filtre.** Funcționalitate prin intermediul căreia Utilizatorii SI SPEG vor putea clasifica/filtra mesajele Email după diferite criterii. Cel puțin următoarele tipuri de clasificare vor fi posibile:
 - a) Clasificarea implicită în mesaje de intrare, mesaje de ieșire, ciorne;
 - b) Clasificarea customizată prin intermediul unor categorii definite de Utilizatorii SI SPEG (Utilizatorul SPEG va dispune de funcționalitate de gestiune a ierarhiei categoriilor de clasificare a mesajelor Email);
 - c) Clasificarea customizată prin intermediul etichetelor atribuite de Utilizatorii SI SPEG mesajelor Email (Utilizatorul SI SPEG va dispune de o funcționalitate de gestiune a ierarhiei de etichete de clasificare a mesajelor Email).

Utilizatorul SI SPEG va putea defini principii de clasificare automată a mesajelor de intrare care corespund unor criterii prestabilite.

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Guvernamentală	Clasificare de securitate
		C4 – Public

- CU01.4: Caut mesaje Email.** Funcționalitate destinată definirii criteriilor căutare globală sau avansată a mesajelor Email. SI SPEG va face uz de mijloace de căutare indexată (*exemplu: prin integrarea unor platforme consacrate de căutare gen Elastic Search, Apache Solr*).

CU02: Gestionez notițe

Caz de utilizate care furnizează totalitatea funcționalităților de gestiune a listei de notițe. Utilizatorul SI SPEG va dispune de funcționalități de creare a notițelor pentru mai multe tipuri de obiecte informaționale ale SI SPEG (ex. mesaje email, contacte, fișiere, altele). La adăugarea unei notițe, utilizatorul SI SPEG va putea redacta textul acesteia, adăuga imagini, fișiere și seta o dată/oră de referință. Aceste funcționalități pot servi ca instrument de gestiune a sarcinilor Utilizatorului SI SPEG. Astfel, dacă va fi indicată o dată/oră, Utilizatorul SI SPEG va putea, la fel, seta ca să primească un mesaj Email de notificare a apropierii momentului respectiv sau cu un interval anumit de timp înaintea lui.

Notițele vor putea fi grupate în mai multe categorii, în funcție de preferințele Utilizatorului SPEG. Notițele pot fi șterse definitiv sau arhivate.


Utilizatorul SPEG va dispune de funcționalități de creare a mesajelor Email pe baza notițelor. În acest caz, tot conținutul notiței va fi preluat într-un mesaj Email în regim de redactare.

În baza notițelor, Utilizatorul SI SPEG va putea, de asemenea, crea un eveniment de Calendar și partaja evenimentul cu alți Utilizatori SI SPEG.

CU03: Gestionez fișiere

Caz de utilizare generic care este accesibil Utilizatorilor SI SPEG, prin intermediul căruia aceștia vor putea încărca și partaja fișiere, crea structuri de directorii, edita documente în regim online și semna electronic documentele. Utilizatorii SI SPEG vor utiliza următoarele funcționalități specifice:

- CU03.1: Creez/Redactez documente.** Funcționalitate destinată Utilizatorilor SI SPEG care oferă posibilitatea de creare a documentelor noi și redactare a documentelor existente în regim online folosind facilitățile oferite de OnlyOffice. Fiind integrat cu platforma de management al documentelor OnlyOffice, SI SPEG va dispune de instrumente pentru editare individuală a documentelor, cât și în comun prin partajarea documentelor cu alți utilizatori. Drepturile de editare în comun a documentelor vor fi atribuite de deținătorul documentului la momentul partajării cu alți utilizatori.
- CU03.2: Semnez documente.** Caz de utilizare care furnizează funcționalități destinate semnări electronice a documentelor gestionate prin intermediul SI SPEG.
- CU03.3: Partajez fișiere.** Caz de utilizare accesibil Utilizatorilor SI SPEG, prin intermediul căruia aceștia vor putea încărca și partaja fișiere prin intermediul mesajelor Email. Fiecare utilizator SI SPEG va avea acces la un spațiu de stocare privat destinat gestiunii fișierelor. SI SPEG va furniza funcționalități pentru organizarea fișierelor în directorii. Atât fișierele, cât și directoriile vor putea fi partajate cu alți utilizatori SI SPEG. Distingem două metode principale de partajare a accesului la aceste resurse:
 - partajarea accesului automat pentru toți destinatarii mesajului email în care sunt inserate link-uri către fișiere/ directorii. Pentru unele tipuri de conversații, utilizatorii SI SPEG vor putea limita accesul la fișierele partajate fie cu permisiunea de redistribuire a acestora sau fără;
 - partajarea customizată a fișierelor/ directoriilor cu specificarea intervalului de timp în care pot fi accesate, parolei de acces și regimului de acces (pentru citire și modificare, doar pentru citire, etc.).

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Guvernamentală	Clasificare de securitate
		C4 – Public

Pentru fiecare fișier sau directoriu partajat, SI SPEG va forma un link unic de acces care va putea fi distribuit de utilizatori atât prin mijloacele de comunicare ale SI SPEG cât și prin alte mijloace alternative (mesagerie instantă, alți furnizori de servicii email, etc.).

Administratorul SI SPEG va dispune de instrumente pentru configurare atât a dimensiunii maxime a fișierelor ce pot fi partajate, cât și a tipurilor de fișiere permise pentru încărcare și partajare.

La nivel tehnic, platforma NextCloud va servi ca spațiu de stocare și gestiune a fișierelor partajate. SI SPEG va integra un API al acestei platforme pentru gestiunea acestor fișiere și configurarea accesului utilizatorilor SI SPEG la ele.

- **CU03.4: Gestionez sistem de fișiere.** Caz de utilizare accesibil Utilizatorilor SI SPEG, prin intermediul căruia aceștia vor putea gestiona sistemul de fișiere aferent contului său utilizator. Acest lucru presupune utilizarea următoarelor facilități: gestiune dosare (creare, redenumire, mutare, ștergere etc.), gestiune fișiere (încărcare, descărcare, redenumire, deschidere/redactare, ștergere etc.). La nivel tehnic, platforma NextCloud va servi ca spațiu de stocare și gestiune a fișierelor Utilizatorului SI SPEG. SI SPEG va integra un API al acestei platforme pentru gestiunea sistemului de fișiere.

CU04: Exploatez calendar


Acest caz de utilizare furnizează funcționalități de gestiune a calendarului personal al utilizatorului SI SPEG. Calendarul reprezintă un instrument destinat planificării evenimentelor de activitate ale Utilizatorului SPEG. Cel puțin următoarele tipuri de înregistrări urmează a fi stocate și gestionate prin intermediul Calendarului furnizat de SI SPEG:

- **Sarcinile utilizatorului** – totalitatea notițelor utilizatorului SI SPEG stocate în calendar pentru care sunt fixate data și ora concretă de îndeplinire și configurat mecanismul de notificare prealabilă;
- **Evenimente planificate** – totalitatea invitațiilor primite de la utilizatorii SI SPEG sau din afară pentru participare la evenimentele create de aceștia. Fiecare eveniment va avea definite data și ora desfășurării, descrierea, fișierele atașate, mecanismul de notificare prealabilă etc.;
- **E-mail-uri programate pentru expediere** – totalitatea mesajelor Email care urmează a fi expediate planificat la o dată și oră concretă;
- **Zile de naștere** ale persoanelor din lista de contacte ale utilizatorului SI SPEG.
- **Sărbători naționale, zile de concediu** și alte zile pe care utilizatorul SI SPEG le marchează ca fiind indisponibil.

Utilizatorul SPEG va dispune instrumente necesare pentru configurarea aspectului vizual al calendarului. Astfel, poate fi configurată atât forma în care sunt afișate evenimentele din calendar, cât și categoriile de evenimente pe care utilizatorul SPEG dorește să le vizualizeze.

Un eveniment de calendar poate fi creat utilizând următoarele strategii:

- Direct din Calendar, folosind opțiunea de adăugare a unui eveniment nou;
- Din formularul de vizualizare al unui mesaj Email;
- Din formularul de vizualizare a unei notițe;
- Dintr-o invitație parvenită din extern la adresa Email a Utilizatorului SI SPEG sau importată dintr-un fișier în format special (exemplu: iCalendar, CSV);

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Governamentală	Clasificare de securitate
		C4 – Public

- Prin sincronizarea datelor cu alte soluții de tip Calendar.

La adăugarea sau modificarea unui eveniment de calendar, utilizatorul SI SPEG va completa titlul acestuia, data și ora evenimentului, descrierea evenimentului, persoanele invitate la eveniment, fișierele/referințele URL atașate, preferințele de notificare etc. Persoanele invitate la eveniment pot fi selectate din lista de contacte a utilizatorului SI SPEG sau adăugate explicit. La salvarea evenimentului de calendar, utilizatorul SI SPEG va avea opțiunea de a expedia o notificare de informare la lista de persoane invitate.

SI SPEG va fi capabil să adauge și actualizeze evenimente de calendar prin sincronizarea evenimentelor de calendar din alte surse externe. Utilizatorul SI SPEG va dispune de funcționalități de adăugare unică a evenimentelor dintr-o sursă externă sau prin configurarea preluării periodice. SI SPEG trebuie să fie capabil să se sincronizeze cu soluția de calendar furnizată de Microsoft Outlook.


CU05: Configurez contul de poștă electronică

Reprezintă un caz de utilizare generic prin intermediul căruia vor fi furnizate totalitatea funcționalităților de configurare a parametrilor de funcționare a serviciului de poștă electronică disponibil Utilizatorului SI SPEG. Cazul de utilizare dat va furniza următoarele funcționalități specifice:

- **CU05.1: Configurez profilul utilizator.** Funcționalitate care oferă Utilizatorului SI SPEG facilități de redactare a datelor profilului personal în SI SPEG și a parametrilor de funcționare a contului de poștă electronică. Cel puțin următoarele tipuri de configurări vor fi accesibile pentru Utilizatorul SI SPEG:
 - a) Redactarea datelor personale.
 - b) Redactarea datelor de contact.
 - c) Definirea intervalului de așteptare până la expedierea mesajului.
 - d) Configurarea semnăturilor prestabilite.
 - e) Setarea semnăturii implicite.
 - f) Alte configurări specifice.
- **CU05.2: Gestionez agenda de contacte.** Funcționalitate prin intermediul căreia Utilizatorul SI SPEG va putea gestiona lista cu toate contactele sale, cât și alte liste de contacte care au fost partajate cu el. SI SPEG va permite crearea de contacte, editarea și ștergerea acestora din agendă.

Utilizatorul SI SPEG va putea ordona și grupa contactele în dependență de necesitățile sale. Pentru fiecare înregistrare din agendă va fi posibil de adăugat date care formează profilul unui contact.

Lista personală de contacte, o grupa anumită de contacte sau o înregistrare particulară pot fi partajate de Utilizatorul SI SPEG cu alți Utilizatori SI SPEG.
- **CU05.3: Configurez aspectul interfață.** Funcționalitate necesară customizării aspectului interfeței utilizator a SI SPEG pentru fiecare Utilizator SI SPEG în parte (*exemplu: aspectul vizual al instrumentelor și datelor afișate în interfața utilizator*). Cel puțin următoarele setări de interfață utilizator vor fi disponibile:
 - a) Selectarea versiunii lingvistice implicite (română sau rusă).
 - b) Numărul maxim de mesaje Email/evenimente de calendar afișate pe o pagină.

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Guvernamentală	Clasificare de securitate
		C4 – Public

- c) Stilul de text prestabilit.
- d) Modul de afișare a panoului de citire al mesajului Email (*exemplu: în fereastră nouă, în panoul din dreapta, în panoul de jos etc.*).
- e) Alte configurări relevante.

- **CU05.4: Gestionez filtre și etichete.** Funcționalitate accesibilă Utilizatorului SI SPEG care oferă posibilitatea gestiunii unei liste organizate ierarhic de etichete. Utilizatorul SI SPEG va avea acces la funcționalități de configurare a mai multor tipuri de filtre care vor fi aplicate în momentul recepționării mesajelor Email.

Un filtru poate fi creat utilizând mai multe proprietăți cum sunt: adresa email de la care este recepționat mesajul, destinatarul mesajului, cuvinte cheie din titlul sau conținutul mesajului, prezența atașamentelor etc. Utilizatorul SI SPEG va putea defini mai multe reguli pentru mesajele Email detectate de filtru (*exemplu: transferul în una din listele de mesaje Email, atribuirea la o categorie, aplicarea uneia sau mai multor etichete, marcarea ca Spam, ștergerea mesajului Email, răspunsul automat etc.*)


SI SPEG va furniza tot spectrul de funcționalități necesare pentru reconfigurarea filtrelor sau eliminarea lor.

- **CU05.5: Gestionez șabloane de mesaje.** Funcționalitate destinată creării și gestiunii ulterioară șabloanelor predefinite de mesaje Email. Utilizatorul SI SPEG va putea crea un șablon în manieră asemănătoare redactării unui mesaj Email. La necesitate, pe lângă textul mesajului, poate fi specificată lista de destinatari și atașate imagini sau fișiere.

Utilizatorul SI SPEG va avea posibilitatea de a iniția redactarea unui mesaj email direct din lista de șabloane disponibile. La fel, la acționarea butonului de creare a unui mesaj Email, dacă sunt disponibile șabloane de mesaje, SI SPEG va sugera utilizatorului 2 opțiuni: creează un mesaj nou sau creează mesajul în baza unui șablon.

- **CU05.6: Activez/dezactivez răspuns automat.** Funcționalitate prin intermediul căreia Utilizatorul SI SPEG va redacta și activa mesajul de răspuns automat în cazul unor evenimente de indisponibilitate pentru o perioadă de timp.
- **CU05.7: Administrez configurări de securitate.** Funcționalitate destinată configurării parametrilor de securitate a contului personal de poștă electronică. Pot fi delimitate următoarele configurări de securitate ce trebuie să fie posibil de definit prin intermediul SI SPEG:

- a) Configurarea preferinței de autentificare și autorizare acces la contul de poștă electronică.
- b) Activarea/dezactivarea autentificării bifactoriale.
- c) Schimbarea parolei de acces la SI SPEG și modalitățile de recuperare;
- d) Gestiunea listei de aplicații client de poștă electronică externă care au acces la contul de poștă electronică, inclusiv a credențialelor de acces SMTP/IMAP pentru fiecare aplicație.
- e) Altele configurări de securitate.

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Governamentală	Clasificare de securitate
		C4 – Public

CU06: Administrez utilizatori si controlul accesului

Caz de utilizare care implementează funcționalitățile destinate gestiunii profilurilor utilizatorilor și drepturilor de acces la resursele și datele SI SPEG. Sistemul Informatic va utiliza mai multe alternative de autentificare a utilizatorilor: login+parolă, semnătură electronică (MPass. SI SPEG va permite activarea și utilizarea mecanismelor de autentificare bifactorială (*exemplu: Email alternativ, SMS, Google Authenticator*)).

Sistemul informatic va furniza funcționalitățile necesare gestiunii grupurilor/rolurilor și drepturilor asociate acestora care urmează să fie ulterior atribuite utilizatorilor autorizați. Drepturile de acces la interfața utilizator și înregistrările bazei de date vor fi definite de grupul/rolul aferent utilizatorului sau explicit pentru fiecare utilizator în parte.

Pentru roluri specifice, drepturile de acces a utilizatorilor la datele și funcționalitățile SI SPEG vor fi atribuite explicit de către utilizatori cu rol administrator.

CU07: Editez profil entitate publică

Reprezintă un caz de utilizare prin intermediul căruia Administratorul SI SPEG sau Administratorul Delegat vor gestiona datele despre entitățile publice conectate la SI SPEG. Adicional la redactarea datelor de profil a autorității publice, Administratorul Delegat va putea configura parametrii specifici de funcționare a SI SPEG pentru toți utilizatorii SI SPEG care aparțin unei entități publice (*exemplu: DNS, mărime spațiu rezervat, cota implicită per cont utilizator etc.*).

Administratorul Delegat va avea posibilitate de manevră în parametrii de configurare, dar în limita setată de Administratorul de Sistem și doar pentru entitățile publice pentru care i-au fost delegate drepturile de administrare.

CU08: Gestionez metadate


Caz de utilizare a SPEG prin intermediul căruia va fi gestionat sistemul de metadate a SI SPEG. Estimativ următoarele categorii de metadate vor putea fi gestionate prin intermediul CU08:

- Clasificatoare oficiale naționale (exemplu: Clasificatorul tipurilor de autorități publice, Clasificatorul tipurilor de funcții publice);
- Clasificatoare/nomenclatoare de interoperabilitate (exemplu: parametri de integrare cu sisteme informatice externe cum sunt: Zimbra, NextCloud, serviciile de platformă MCloud etc.);
- Clasificatoare/nomenclatoare interne (exemplu: etichetele și mesajele interfeței utilizator în cele 2 versiuni lingvistice, variabile de sistem, parametri ai interfeței utilizator, parametri de configurare a sistemului informatic etc.).

CU09: Gestionez alerte

Caz de utilizare care implementează funcționalități destinate Administratorului sistemului pentru gestiunea alertelor de securitate identificate în regim automat de SI SPEG în baza regulilor configurate. Acest caz de utilizare va furniza un instrument de verificare și rezolvare a incidentelor de securitate prin aplicarea unor reguli suplimentare în utilizarea SI SPEG, în dependență de caz și pentru segmente anumite de utilizatori (exemplu: blocarea accesului utilizatorului în sistem, restricționarea accesului de pe o adresă IP, limitarea numărului de conexiuni într-un interval de timp etc.).

Administratorul sistemului va decide dacă este cazul să aplice restricționări pentru utilizarea SI SPEG în dependență de severitatea incidentului. Pentru fiecare alertă de securitate, Administratorul va avea

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Governamentală	Clasificare de securitate
		C4 – Public

posibilitatea să introducă o mențiune cu privire la rezolvarea ei și să aplice una sau mai multe reguli. La aplicarea unei reguli poate fi specificată perioada de timp pentru care regula va fi activă.

CU10: Configurez SPEG

Reprezintă un caz de utilizare care furnizează funcționalitățile necesare configurării parametrilor de funcționare a SI SPEG. Trebuie de menționat faptul că SI SPEG trebuie să fie un sistem configurabil și adaptarea lui la necesitățile curente ale utilizatorilor și cadrului legal în vigoare trebuie să se facă prin intermediul mecanismelor de configurare fără a fi necesară intervenția în codul program, compilarea acestuia și activități de desfășurare repetată a sistemului informatic.

Administratorul de Sistem va avea acces la configurarea a cel puțin următoarele tipuri de parametri:

- **Parametri de funcționare a sistemului de poștă electronică** dedicat autorității publice (exemplu: parametri de configurare SMTP și IMAP, configurări anti spam și antivirus, durata de valabilitate a sesiunii, configurarea metodelor de autentificare și autorizare acces în cadrul SI SPEG, parametri de integrare cu sistemele informatice externe etc.).
- **Parametri de configurare a conturilor de poștă electronică** a funcționarilor autorităților publice (exemplu: spațiul maxim disponibil pentru un cont, activarea/dezactivarea unor funcționalități destinate gestiunii contului de poștă electronică, interval de așteptare la nivel de profil al utilizatorului până la expedierea mesajului etc.).

CU11: Monitoring operațional si diagnostica


Caz de utilizare complex prin intermediul căruia rolurile administrative ale SI SPEG vor avea acces la funcționalitățile de monitorizare a parametrilor de funcționare a SI SPEG, diagnostic și depanare a problemelor tehnice apărute în procesul exploatării SI SPEG.

Cazul dat de utilizare va furniza funcționalități destinate generării rapoartelor statistice predefinite și ad-hoc privind evenimentele de exploatare a SI SPEG. Rapoartele în cauză sunt utile pentru analiza proceselor desfășurate, bazei informaționale a sistemului informatic, performanței activității utilizatorilor autorizați, permițând anticiparea problemelor de securitate informațională.

CU12: Schimb date cu sisteme externe

Caz de utilizare care va furniza funcționalitățile necesare SI SPEG pentru schimbul de date cu sisteme informatice externe sau integrarea cu serviciile guvernamentale de platformă. Acest schimb de date se referă la expunerea sau consumarea interfețelor destinate schimbului reciproc de date (recepționarea datelor din surse externe, expedierea datelor către sisteme informatice externe și schimbul bidirecțional al datelor). Următoarele sisteme informatice externe urmează a fi integrate cu SI SPEG:

- componentele interne ale infrastructurii SI SPEG, prin intermediul REST API (*exemplu: Zimbra, NextCloud, OnlyOffice*);
- serviciile de platformă (*MPass, MSign, MLog, MNotify, MPower*) urmează a fi integrate direct prin intermediul API-urilor expuse de acestea;
- aplicațiile client de poștă electronică de pe dispozitivele mobile sau calculatoare personale ale Utilizatorilor SI SPEG prin intermediul protocoalelor necesare (*exemplu: SMTP, IMAP*);
- sistemele de gestiune a resurselor umane ale autorităților publice.

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Guvernamentală	Clasificare de securitate
		C4 – Public

CU13: Expediez notificări

Caz de utilizare care furnizează funcționalitățile de notificare a rolurilor specifice ale SI SPEG. Notificările vor fi expediate asigurând-se acces direct (dacă e cazul) la formularul electronic, evenimentul de business care a generat notificarea.

SI SPEG va genera și expedia automat utilizatorilor autorizați notificări aferente oricărui eveniment de business care necesită implicarea acestora.

CU14: Jurnalizez evenimente

Reprezintă un caz de utilizare prin care va fi efectuată jurnalizarea evenimentelor de business generate de componentele funcționale ale SI SPEG. Orice eveniment generat în cadrul proceselor de business implementate în cadrul SI SPEG vor fi jurnalizate și salvate în tabelele corespunzătoare ale Bazei de Date.

Mecanismul de jurnalizare va fi dezvoltat în baza standardelor și bunelor practici implementate în industrie. Sistemul informatic va livra funcționalități de configurare a strategiei de jurnalizare a evenimentelor de business, inclusiv: categoriile de evenimente de business supuse jurnalizării, perioada calendaristică de jurnalizare (determinată sau nedeterminată) etc.

Pentru evenimentele de business critice sau sensibile, jurnalizarea se va efectua suplimentar prin intermediul serviciului de platformă MLog.


CU15: Execut proceduri automate

Caz de utilizare complex care furnizează funcționalitățile de declanșare și funcționare în regim automat a unui șir de funcționalități ale SI SPEG în vederea utilizării raționale a resurselor server, lansarea serviciilor specifice funcționării SI SPEG și furnizării la momentul oportun a datelor pentru utilizatorii autorizați. CU15 este extins de următoarele cazuri de utilizare:

- **CU15.1: Execut job-uri de sistem.** Caz de utilizare care implementează funcționalități aferente îndeplinirii planului de execuție a sarcinilor de sistem configurate în SI SPEG.
- **CU15.2: Generez alerte de securitate.** Un tip specific de procedură automată pe care trebuie să o furnizeze SI SPEG se referă la asigurarea securității prin implementarea unor mecanisme de monitorizare în fundal a activității utilizatorilor. Aceste proceduri, în baza comportamentului utilizatorului, vor scoate în evidență activitățile suspecte (ex. autentificare la intervale de timp scurte din regiuni geografic îndepărtate, altele). SI SPEG va expedia notificări Administratorul sistemului cu privire la aceste alerte de securitate.

Distingem două tipuri de incidente de securitate din punct de vedere a căii de rezolvare a acestora: cele care sunt rezolvate automat (în baza procedurilor predefinite în sistem) și cele care necesită implicarea administratorului pentru a decide procedura optimă de rezolvare care va fi aplicată.

- **CU15.3: Restricționez accesul la contul utilizatorului.** Caz de utilizare al SI SPEG care reprezintă acțiunea de restricționare acces la funcționalitățile SI SPEG pentru conturile de utilizator pentru care au fost înregistrate activități sau acțiuni suspecte. Blocarea automată a contului de utilizator survine în urma procedurilor automate declanșate de SI SPEG, și care rulează în fundal, pentru identificarea și prevenirea riscurilor care pot duce la compromiterea securității SI SPEG.
- **CU15.4: Monitorizez activitate utilizatori.** Caz de utilizare care furnizează funcționalități de monitorizare a activității tuturor părților care interacționează cu SI SPEG (utilizatori, aplicații client, sisteme informatice externe) cu scopul de a înregistra acțiunile critice și identifica

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Governamentală	Clasificare de securitate
		C4 – Public

activități suspecte în baza cărora vor fi expediate alerte de securitate sau va fi restricționat în regim automat accesul utilizatorilor la SI SPEG.

A1.3. Arhitectura SI SPEG

SI SPEG trebuie să furnizeze o interfață WEB, accesibilă prin intermediul unui explorator Internet de largă utilizare (MS Internet Explorer/MS Edge, Mozilla Firefox, Opera, Google Chrome sau Safari). Din punct de vedere funcțional se va dezvolta o soluție fiabilă și scalabilă atât în cazul creșterii numărului de utilizatori concurenți sau, cât și în cazul creșterii volumului de informație gestionată de acesta.

La baza SI SPEG va sta o arhitectură orientată la servicii multinivel (care exclude interacțiunea directă a aplicației cu baza de date) bazată pe tehnologiile WEB adecvate timpului. Întru asigurarea unui nivel adecvat al securității informaționale, sistemul informatic livrat trebuie să permită realizarea de conexiuni securizate între stațiile client și serverul de aplicație pentru asigurarea siguranței informației expediate (utilizându-se conexiuni VPN și sesiunilor TLS/SSL).

SI SPEG va fi desfășurat și va funcționa în cadrul platformei guvernamentale MCloud. Întru asigurarea obiectivelor înaintate soluției informatice, la proiectarea, dezvoltarea și implementarea SI SPEG trebuie să se țină cont de arhitectura descrisă în figura 3.

Arhitectura descrisă în diagrama de componente a figurii 3 este una de nivel înalt și indicativă. Ea descrie elementele principale ale SI SPEG și modalitatea de interacțiune între acestea. Furnizorul, în comun cu experții STISC vor elabora o arhitectură detaliată a SI SPEG în cadrul activităților de elaborare a Conceptului SI SPEG. Numai după identificarea și aprobarea soluției de arhitectură a SI SPEG Furnizorul va putea demara activitățile de dezvoltare a SI SPEG.

După cum se vede în figura 3, soluția de cooperare a resurselor pentru asigurarea funcționalității SIA SPEG constă din 8 categorii de noduri distincte:

- **MCloud** – infrastructura TIC a platformei tehnologice guvernamentale comune care formează cloud-ul guvernamental (MCloud) unde sunt găzduite, de regulă, toate sistemele informatice ale AP din Republica Moldova și unde urmează a fi găzduit SI SPEG. Trebuie de menționat faptul că SI SPEG va consuma serviciile de platformă, iar integrarea cu sistemele informatice externe se va realiza preponderent prin intermediul platformei de interoperabilitate guvernamentale MConnect.
- **Calculatoarele client** – calculatoarele, de la care se va accesa de către utilizatorii autorizați (în funcție de drepturi și roluri) funcționalitățile SI SPEG.

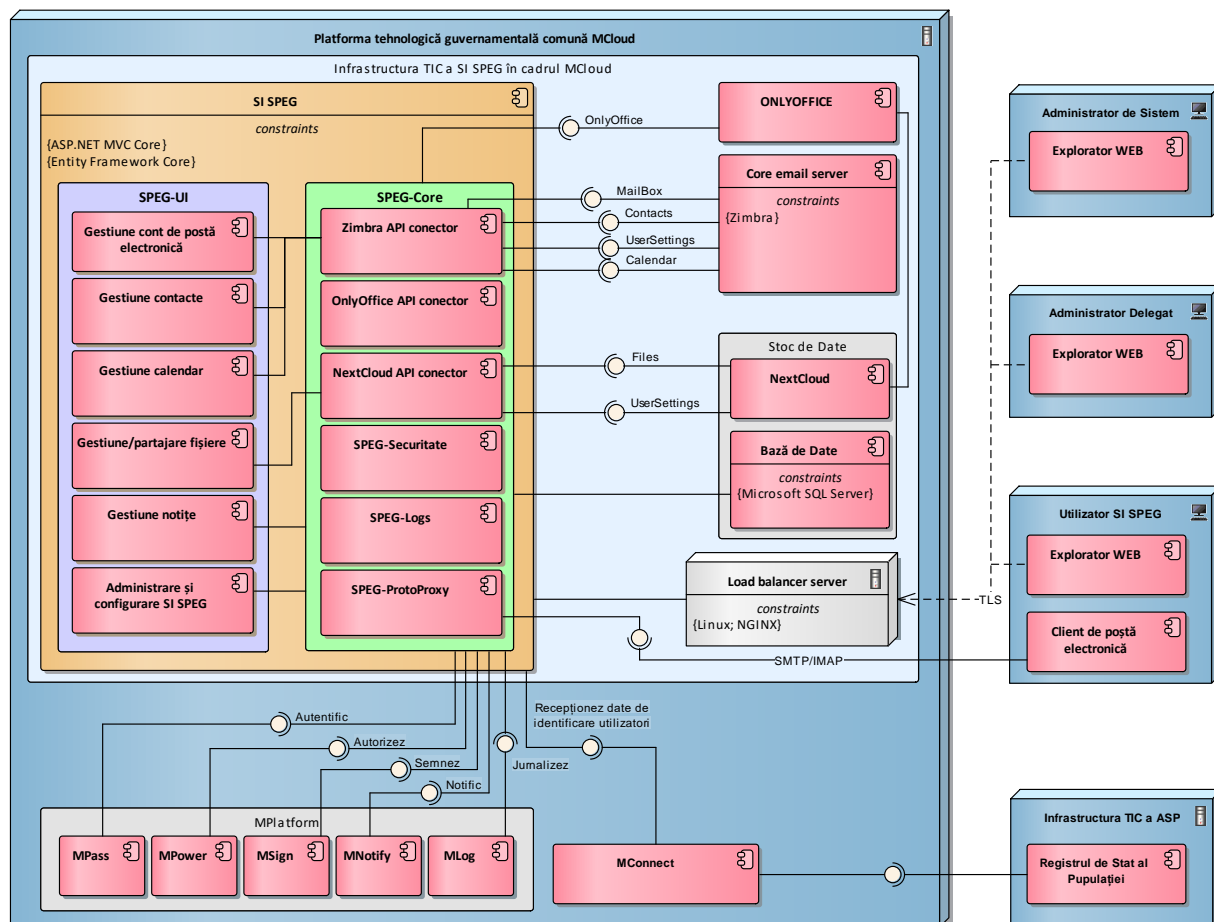



Figura 3. Arhitectura indicativă a SI SPEG.

Conform diagramei de desfășurare și componente din figura 3, SI SPEG constă din 7 componente de bază:

- **Interfața utilizator** – componenta FrontEnd a SI SPEG prin intermediul căreia utilizatorii autorizați, în funcție de rolurile deținute, au acces la serviciile de poștă electronică și facilitățile de administrare a SI SPEG.
- **SPEG-Core** – componentă BackEnd care furnizează setul de servicii și interfețe accesibile utilizatorilor autorizați și sistemelor informatice externe. Această componentă este responsabilă inclusiv de integrarea cu serviciile de platformă și interoperabilitatea internă între componentele SI SPEG.
- **Core Email server** – componentă funcțională responsabilă de furnizarea funcționalităților de bază a serviciului de poștă electronică. În calitate de soluție core Email server va fi utilizată Zimbra care va expune API-uri specializate către SPEG-Core.
- **OnlyOffice** – componentă funcțională responsabilă de furnizarea funcționalităților necesară redactării online individuale și în comun a documentelor.
- **Stocul de date** – componenta SI SPEG care răspunde de stocarea datelor aferente SI SPEG. În acest sens e vorba atât de baza de date, cât și de fișierele cu care operează utilizatorii autorizați ai SI SPEG.
- **Balansorul SI SPEG** – destinat balansării încărcării instanțelor server în baza căreia va funcționa SI SPEG.

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Governamentală	Clasificare de securitate
		C4 – Public

Pentru implementarea unui șir de funcționalități, SI SPEG va consuma un șir de servicii de platformă și API-uri furnizate de sisteme informatice guvernamentale și externe după cum urmează:

- **Serviciul Autentic** furnizat de serviciul guvernamental de platformă MPass în scopul implementării procedurilor de autentificare a utilizatorilor prin intermediul semnăturii electronice sau semnăturii mobile;
- **Serviciul Autorizez** furnizat de serviciul guvernamental de platformă MPower în scopul verificării împuternicirilor utilizatorului autorizat în utilizarea serviciului de poștă electronică guvernamentală.
- **Serviciul Semnez** furnizat de serviciul guvernamental de platformă MSign în scopul implementării mecanismului de aplicare/verificare a semnăturii electronice a documentelor sau mesajelor Email gestionate în cadrul SI SPEG;
- **Serviciul Notific** furnizat de serviciul guvernamental de platformă MNotify în scopul implementării funcționalității de notificare a utilizatorilor autorizați în cazul producerii unor evenimente de business specifice.
- **Serviciul Jurnalizez** furnizat de serviciul guvernamental de platformă MLog pentru jurnalizarea evenimentelor de business specifice.
- **Serviciul Core Email** furnizat de Zimbra prin intermediul unor interfețe specifice destinate accesării funcționalităților accesibile prin intermediul Zimbra:
 - MailBox – accesarea funcționalităților de poștă electronică;
 - Contacte – accesarea funcționalităților de gestiune și utilizare a agendei de contacte;
 - Calendar – accesarea funcționalităților de gestiune și utilizare a calendarului de evenimente;
 - Gestiune utilizatori – accesarea funcționalităților de gestiune și a utilizatorilor și conturilor de poștă electronică;
- **Serviciul NextCloud** care reprezintă o suită de software client-server pentru crearea și utilizarea serviciilor de găzduire a fișierelor prin intermediul serviciilor de bază oferite
 - Gestiune fișiere
 - Gestiune utilizator
 - Gestiune obiecte partajate
- **Serviciul OnlyOffice** care reprezintă o suită de software client-server foarte apropiată de funcționalitățile Microsoft Office pentru vizualizarea și redactarea documentelor cu extensie MS Office.
- **Serviciul Recepționez date de identificare utilizatori** utilizat pentru actualizarea automatizată a datelor de profil a utilizatorilor de poștă electronică guvernamentală.

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Governamentală	Clasificare de securitate
		C4 – Public

Anexa 2. Cerințe tehnice

Compartimentul dat expune cerințele nefuncționale de care trebuie să se țină cont la etapele de proiectare, dezvoltare, implementare și operare a SI SPEG.

A2.1. Cerințe față de documentația de însoțire

Nr.	Categorie cerință	Descriere cerință
1.	Documente destinate utilizatorilor finali	Dezvoltatorul va elabora și prezenta următoarele documente pentru utilizatorii finali ai SI SPEG: <ol style="list-style-type: none"> Ghid interactiv inclus în interfața utilizatorului din SI SPEG și ajustat la rolul utilizatorului (Utilizator SPEG, Administrator delegat, Administrator de Sistem). Manualele utilizatorului descărcabile în format PDF pentru Utilizator SPEG, Administrator delegat, Administrator de Sistem etc. Toată documentația destinată utilizatorului final va fi perfectată în limba română.
2.	Documentație tehnică	Furnizorul va elabora și prezenta următoarele documente tehnice: <ol style="list-style-type: none"> Concept de nivel înalt (HLD) al SI SPEG Documentația pentru arhitectura SI SPEG (inclusiv descrierea modelelor în limbaj UML, cu un nivel suficient de detaliere a arhitecturii sistemului). Strategia testării (inclusiv scenariile de testare). Codul sursă compilabil și documentat pentru aplicațiile, componentele și testele unitare dezvoltate în cadrul proiectului. Toată documentația tehnică va fi în limba română.

A2.2. Cerințe față de instruirea utilizatorilor

Nr.	Categorie cerință	Descriere cerință
1.	Sesiuni de instruire	Furnizorul va realiza sesiuni de instruire la sediul STISC și sesiuni on-line pentru utilizatori cu rol administrator.
2.	Materiale instructive	Furnizorul urmează să pregătească și livreze totalitatea documentelor necesare desfășurării în bune condiții a instruirii utilizatorilor.
3.	Limba de instruire	Conținutul cursului de instruire și a materialelor de instruire vor fi prezentate în română.


	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Guvernamentală	Clasificare de securitate
		C4 – Public

A2.3. Drepturi de proprietate

Nr.	Categorie cerință	Descriere cerință
1.	Licență software perpetuă	Furnizorul va acorda STISC dreptul nelimitat/total asupra soluției dezvoltate, inclusiv de exploatare și dezvoltare ulterioară a SI SPEG și pentru toate componentele software incluse fără vreo limitare de timp, locație și funcționalitate oferită.
2.	Dreptul de redistribuire	Furnizorul va acorda STISC dreptul de redistribuire a soluției. Deși STISC nu intenționează să redistribuie soluția pe o scară largă, acesta totuși prevede necesitatea transferului soluției software către alte agenții de stat, de exemplu în cazul unei eventuale reorganizări. De asemenea, STISC ar putea să aibă posibilitatea să re-amplaseze întreaga platformă e-Guvern.
3.	Drepturi depline asupra datelor	STISC păstrează drepturile depline asupra datelor create cu ajutorul acestei soluții.
4.	Formatul open data	SI SPEG păstrează datele în format deschis sau include mecanisme de extragere a datelor din sistem în format deschis, permițând astfel transferul/migrarea datelor într-un alt sistem informatic.

A2.4. Cerințe față de arhitectură

Nr.	Categorie cerință	Descriere cerință
1.	Standarde deschise	Arhitectura SI SPEG va fi bazată pe standarde deschise relevante și nu va utiliza standarde proprietare. Arhitectura SI SPEG trebuie conceptualizată utilizându-se o viziune integrată, bazată pe bunele practici ale industriei TIC (exemplu: utilizând abordarea TOGAF 9.1).
2.	Arhitectură orientată pe servicii	SI SPEG va fi implementat în baza unei Arhitecturi orientate pe servicii. SI SPEG trebuie să fie implementat în baza unei arhitecturi modulare bazată pe componente reutilizabile și interfețe abstracte care vor impune implementarea unei arhitecturi multinivel cu o clară delimitare a nivelelor arhitecturale. Componentele de sistem trebuie să fie relativ independente și să interacționeze între ele prin intermediul unor interfețe dedicate.
3.	Mediul de găzduire	SI SPEG nu va include componente hardware și la finalizare va fi găzduită în cadrul platformei guvernamentale comune MCloud.
4.	Mediul de rulare	SI SPEG va rula pe motorul container Docker și nu va depinde de instanța specifică a sistemului de operare gazdă. Crearea imaginilor container va fi un proces automatizat (a se accesa următorul link pentru detalii: https://docs.docker.com/develop). Rulată într-un mediu bazat pe containere, aplicația trebuie să fie elastică, inclusiv în cazul adăugării/eliminării instanțelor container (peste instanțele minim necesare pentru disponibilitatea înaltă), modificarea configurațiilor și parametrilor de sistem nu va avea nici

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Governamentală	Clasificare de securitate
		C4 – Public

Nr.	Categorie cerință	Descriere cerință
		un impact asupra activității în derulare, cum ar fi sesiunile active, cereri etc.
5.	Instanțe multiple	Arhitectura soluției va asigura un grad înalt de disponibilitate la implementarea noilor versiuni și posibilitatea rulării simultane a câtorva instanțe.
6.	Compatibilitatea exploratorului WEB	SI SPEG va fi compatibil cu ultimele două versiuni majore (care vor fi luate în considerare în momentul acceptării sistemului) ale exploratoarelor WEB: Chrome, Safari, FireFox și Edge.
7.	Model detaliat al datelor	Modelul de date detaliat al SI SPEG va fi descris în totalitate într-o schemă de date electronice (exemplu: utilizând limbajului DDL pentru bazele de date relaționale). Furnizorul va coordona în prealabil formatul detaliat al schemei modelului de date cu Clientul.

A2.5. Cerințe de integrare

Nr.	Categorie cerință	Descriere cerință
1.	Integrarea cu serviciile de platformă guvernamentale	Următoarele servicii guvernamentale urmează a fi integrate: <ul style="list-style-type: none"> • MPass - pentru autentificarea utilizatorilor; • MSign - pentru semnarea electronică a mesajelor Email expediate și documentelor atașate; • MNotify - pentru notificarea utilizatorilor despre evenimente generate de sistem; • MLog - pentru jurnalizarea acțiunilor/evenimentelor de business și extragerea statisticilor de utilizare a serviciilor expuse de SI SPEG. • MPower - pentru verificarea împuternicirilor de utilizare a poștei electronice guvernamentale.
2.	Integrare cu sisteme externe	SI SPEG trebuie să fie capabil să se integreze cu următoarele sisteme informatice externe: <ul style="list-style-type: none"> • Registrul de Stat al Populației; • Programe client de poștă electronică; • Programe calendar destinate planificării și gestiunii evenimentelor.

A2.6. Cerințe de performanță


Nr.	Categorie cerință	Descriere cerință
1.	Procesarea asincronă	Si SPEG va utiliza procesarea asincronă pentru generarea intrărilor-ieșirilor ori de câte ori este posibil.

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Guvernamentală	Clasificare de securitate
		C4 – Public

Nr.	Categorie cerință	Descriere cerință
2.	Utilizatori concurenți	Sarcina și performanța standard a sistemului va fi garantată pentru 10000 utilizatori umani sau aplicații externe de poștă electronică concurenți.
3.	Timpul de reacție	Timpul de reacție pentru funcțiile SI SPEG va fi de până la 3 (trei) secunde. Furnizorul va enumera excepțiile, dacă este cazul, și le va discuta/conveni cu STISC la etapa de analiză și proiectare.
4.	Indicatori de performanță	<p>SI SPEG va măsura și va expune în interfața Administratorului de Sistem principalii indicatori de performanță. Furnizorul va propune lista indicatorilor și îi va discuta/conveni cu STISC.</p> <p>Furnizorul va executa teste interne de performanță a SI SPEG conform planului de testare a performanței (stress și load testing) agreat cu STISC.</p> <p>La acceptanța finală, STISC va efectua independent testarea de performanță a SI SPEG și va expedia către Furnizor rezultatele pentru informare sau remediere a problemelor de performanță depistate.</p>

A2.7. Cerințe pentru interfața utilizator

Nr.	Categorie cerință	Descriere cerință
1.	Interfață multilingvă	<p>SI SPEG va furniza interfață utilizator multilingvă, prin formate specifice tipului de date (exemplu: data, ora, intervale de timp, numere etc.).</p> <p>Interfața FrontEnd a SI SPEG va fi livrată în versiunile română și rusă. Interfața BackEnd-ul a SI SPEG va fi livrată cel puțin în versiunea română.</p> <p>Versiunea implicită pentru utilizatorul final va fi româna.</p>
2.	Accesibilitate interfață utilizator	<p>Interfața utilizatorului va conformă cu cel puțin Nivelul AA al Ghidului privind accesibilitatea conținutului web 2.1.</p> <p>https://www.w3.org/TR/WCAG21/</p>
3.	Design receptiv/adaptiv	<p>Interfața utilizatorului se va adapta automat la diferite rezoluții de ale dispozitivelor utilizatorilor SI SPEG. Lățimea minimă a zonei de afișare este 480px.</p> <p>Interfața utilizator a SI SPEG va fi implementată utilizând tehnologiile aplicației web progresive (PWA) și va fi funcțională pe dispozitivele mobile și tactile.</p>
4.	Suport contextual	Elementele interfeței utilizator a SI SPEG vor include Sfaturi și Sugestii pentru compartimentele furnizate utilizatorilor autorizați.
5.	Suport utilizatori	Toate paginile vor include contactele de asistență pentru utilizatori.

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Governamentală	Clasificare de securitate
		C4 – Public

Nr.	Categorie cerință	Descriere cerință
6.	Marcaje	Toate paginile principale ale SI SPEG vor fi putea fi marcate (exemplu: mesaj email, eveniment de agendă, fișier partajat etc.), iar utilizatorul trebuie să aibă posibilitatea să acceseze paginile marcate mai târziu. Paginile care pot fi marcate vor fi determinate la etapa de analiză.
7.	URL prietenoase	SI SPEG va utiliza URL-uri care sunt ușor de utilizat pentru accesarea compartimentelor acestuia.

A2.8. Cerințe de mentenanță

Nr.	Categorie cerință	Descriere cerință
1.	Jurnale de sistem	SI SPEG va înregistra acțiunile și evenimentele într-o manieră structurată. Jurnalizarea va fi configurabilă și bazată pe un cadru de jurnalizare extensibil (exemplu: log4net, nlog etc.). Cadrul de jurnalizare va susține cel puțin formatul JSON și următoarele ținte: consolă, fișiere de rulare, UDP și HTTP POST.
2.	Nivele de jurnalizare și înregistrările jurnalului de evenimente	SI SPEG va diferenția evenimentele și acțiunile pe care le înregistrează după cel puțin următoarele nivele: Critic, Eroare, Avertizare, Info, Depănare. Evenimentele de nivel Critic și Eroare vor fi înregistrate doar pentru eroarea nerecuperabilă care necesită intervenția umană. Înregistrările din jurnalul evenimentelor vor include cel puțin: <ul style="list-style-type: none"> • tipul evenimentului; • timestamp-ul (marca de timp) când evenimentul a avut loc; • nivelul evenimentului; • componenta de sistem care a generat evenimentul; • utilizatorul/agentul utilizatorului, IP care a declanșat evenimentul; • identificatorul obiectului informațional afectat; • detalii textuale despre evenimentul produs.
3.	Închidere grațioasă	SI SPEG va implementa închiderea grațioasă și anume închiderea unei instanțe de container a aplicației nu va afecta activitățile în derulare, cum ar fi sesiunile active, cererile, jurnalele evenimentelor etc.
4.	Codul sursă	Furnizorul va livra codul sursă pentru componentele SI SPEG care nu sunt disponibile ca produse comerciale autonome de la părți terțe. Codul sursă va utiliza managerii de pachete pentru dependențele de bibliotecile terțe. Toate soft-urile adiționale necesare vor fi incluse în definiția imaginii containerului și bazate pe repoziitoriul public de containere.

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Guvernamentală	Clasificare de securitate
		C4 – Public

Nr.	Categorie cerință	Descriere cerință
5.	Implementare	Furnizorul va aplica procedura de implementare și instrumentele necesare. Procedura de implementare va acoperi toate condițiile înainte de a iniția instalarea sistemului. Implementarea va fi automatizată și va include inițializarea bazei de date.
6.	Actualizări de sistem	Actualizările de sistem vor fi automatizate, inclusiv scripturile de upgrade/downgrade a bazei de date sau codul. Pentru a permite rularea actualizărilor în mediul de producție, se recomandă operarea unor modificări minore la nivelul bazei de date.

A2.9. Cerințe de securitate

Nr.	Categorie cerință	Descriere cerință
1.	Arhitectură securizată	<p>SI SPEG va avea un design securizat și se va conforma cu toate cerințele specificate în HG 201 din 28.03.2017 (https://www.legis.md/cautare/getResults?doc_id=98644&lang=ro).</p> <p>Furnizorul va prezenta documentația care descrie designul și dovezile confirmative privind securizarea acestuia.</p> <p>Furnizorul va coordona cu STISC formatul documentației, documentelor confirmative și lista cerințelor cu care urmează să se conformeze.</p> <p>STISC poate să se asigure de funcționalitatea caracteristicilor de securitate ale SI SPEG conform cerințelor prestabilite, prin efectuarea de o terță parte a testelor respective</p>
2.	Principiul privilegiilor minime	<p>Componentele SI SPEG se vor baza pe principiul privilegiilor minime și vor rula în regim de privilegii limitate în cadrul modelului drepturilor sistemului de operare.</p> <p>Documentația va evidenția nivelul necesar de privilegiu pentru fiecare componentă a SI SPEG și motivele care fac necesară utilizarea nivelului de acces propus.</p>
3.	Secrete și adrese	Datele secrete (parole, cheile și certificatele private, șirurile de conexiune etc.) și adresele serviciilor externe vor fi delimitate clar în documentația de confirmare și ușor modificabile prin scripturi automatizate.
4.	Canale de comunicare securizate	Toată comunicarea SI SPEG cu sistemele sau utilizatorii externi va avea loc prin canale de comunicare criptate.
5.	Autentificare utilizatori	<p>SI SPEG va utiliza MPass în calitate de mecanism de autentificare a utilizatorilor în cazul exploatării de către utilizatorii de poștă electronică a interfeței Web.</p> <p>Pentru cazurile utilizării unor aplicații client de poștă electronică prin intermediul SMTP/IMAP va fi utilizat un alt mecanism de autentificare</p>



Nr.	Categorie cerință	Descriere cerință
		și autorizare acces care urmează a fi definit în procesul de proiectare a SI SPEG.
6.	Minimizarea stocării datelor cu caracter personal	SI SPEG va minimiza datele identificabile personal care sunt stocate și trebuie să fie conform cu cerințele de procesare a datelor cu caracter personal specificate în HG 1123 din 14.12.2010 (https://www.legis.md/cautare/getResults?doc_id=16012&lang=ro). Furnizorul va coordona cu STISC lista cerințelor de protecție a datelor cu caracter personal cu care urmează să se conformeze.
7.	Eliminare vulnerabilități	SI SPEG va include controale de securitate pentru toate componentele sale pentru cel puțin OWAS top 10 vulnerabilities https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
8.	API health-check	SI SPEG va expune pregătirea și API-ul health-check prin solicitări HTTP GET. Health-checkul va verifica starea a cât mai multor componente ale SI SPEG posibile. În cazul identificării unei erori, va fi trimis un mesaj de eroare lizibil pentru om.
9.	Gestiune roluri	SI SPEG va dispune de funcționalitate de gestiune a rolurilor utilizatorilor, inclusiv adăugare, retragere și configurare rol.
10.	Expirare sesiune	SI SPEG va include un mecanism de expirare a sesiunilor care îi va cere utilizatorului să se autentifice din nou după o anumită perioadă în care a fost inactiv. Perioada de inactivitate va fi configurabilă, iar cea implicită este de 15 minute.
11.	Validare intrări	Toate datele de intrare vor fi validate atât de client, cât și de server.
12.	Conținutul utilizatorului	Conținutul utilizatorului poate fi captat doar în format text. SI SPEG va interzice înserarea caracterelor speciale utilizate pentru formatare și marcarea conținutului web special. Toate caracterele UNICODE vor putea fi inserate/vizualizate în cadrul componentele SI SPEG.
13.	Încercare acces neautorizat	Când SI SPEG înregistrează încercări de accesare neautorizate, acesta va: <ul style="list-style-type: none">• atribui acestei încercări cel puțin nivelul EROARE;• transmite utilizatorilor un mesaj de avertizare că accesul nu este autorizat și abuzul va fi investigat.
14.	Integritate date	Furnizorul va asigura integritatea datelor prin oferirea unei soluții adecvate pentru prevenirea activităților interne neautorizate (exemplu: ștergerea mesajului Email direct din baza de date).

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Guvernamentală	Clasificare de securitate
		C4 – Public

A2.10. Cerințe de asistență și garanție

Nr.	Categorie cerință	Descriere cerință
1.	Asistență	Furnizorul va oferi STISC asistența tehnică necesară în perioada de garanție (pe parcursul a 12 luni de la punerea în producție a SI SPEG).
2.	Garanție	<p>În perioada de garanție Furnizorul va:</p> <ul style="list-style-type: none"> • elimina toate defectele raportate de STISC; • va soluționa toate incidentele raportate de STISC în conformitate cu ANS convenite. <p>Notă: Pentru o soluție temporară, timpul de răspuns și soluționare nu va depăși 24 ore în cazul erorilor non-critice și 4 ore în cazul erorilor critice.</p> <p>Incidentele vor fi soluționate în termen de 4 zile lucrătoare pentru erorile non-critice și de 2 zile lucrătoare pentru erorile critice începând cu momentul escaladării. În cazul erorilor critice la fiecare ora va fi furnizat un raport de progres.</p>

A2.11. Cerințe de migrare a datelor


Nr.	Categorie cerință	Descriere cerință
1.	Obiectivele migrării datelor	Furnizorul trebuie să implementeze în cadrul SI SPEG mecanism de import a conturilor utilizatorilor serviciului curent de poștă electronică guvernamentală utilizând facilități de tip sync/resync (discovery). }
2.	Metodologia de migrare	Furnizorul trebuie să propună către STISC metodologia de migrare a datelor către SI SPEG.
3.	Responsabilitățile Furnizorul	<p>Pe parcursul implementării procedurii de migrare și populare a datelor Furnizorul este responsabil pentru:</p> <ul style="list-style-type: none"> • definirea metodologiei utilizate în procesul de migrare și populare a datelor; • furnizarea mecanismelor software destinate migrării și populării datelor; • definirea criteriilor de reconciliere a datelor migrate și populate; • popularea SI SPEG cu date primare în baza mecanismului implementat; • identificarea și soluționarea excepțiilor/erorilor pe parcursul procesului de migrare și populare a datelor.

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Governamentală	Clasificare de securitate
		C4 – Public

Nr.	Categorie cerință	Descriere cerință
4.	Reconcilierea datelor	<p>Toate activitățile de migrare și populare inițială a SI SPEG cu date trebuie să fie efectuate în mediul de operare controlat de STISC. Datele nu vor părăsi niciodată infrastructura TIC a STISC.</p> <p>În procesul migrării Furnizorul se va confirma politicii de securitate a STISC.</p> <p>Furnizorul va demonstra corectitudinea instrumentarului de migrare și populare inițială cu date a SI SPEG specialiștilor STISC.</p>


A2.12. Cerințe de asigurare calitate

Nr.	Categorie cerință	Descriere cerință
1.	Activitățile cheie	<p>Furnizorul va organiza testarea de acceptanță a sistemului. Testarea urmează a fi efectuată după finisarea fiecărei iterații (dacă e cazul) și la acceptanța finală a SI SPEG. În acest scop, acesta va executa cel puțin următoarele activități:</p> <ul style="list-style-type: none"> • definirea strategiei de testare și a procedurii de testare; • pregătirea planurilor detaliate de testare, inclusiv scenarii de testare; • recepționarea erorilor depistate și înlăturarea acestora; • pregătirea planului cu rezultatele finale ale testării, inclusiv statutul tuturor erorilor identificate. <p>Acoperirea cu unit teste pentru capabilitățile SI SPEG va fi minim 90%.</p>
2.	Livrabile	<p>Furnizorul va livra spre coordonare și acceptare către STISC planul de testare de acceptanță.</p> <p>Furnizorul va livra spre coordonare și acceptare către STISC scenariile de testare pentru toate categoriile de teste (unit testing, integration testing, stress testing, load testing.etc.).</p> <p>Furnizorul va livra spre coordonare și acceptare către STISC raportul cu privire la rezultatele testării SI SPEG.</p>
3.	Criteriile de acceptanță	<p>Furnizorul va efectua în comun cu reprezentanții STISC toate testele planificate conform Planului de testare. Rezultatele finale ale acestora trebuie să fie acceptate de STISC.</p> <p>Acceptarea rezultatului testelor se va face dacă se vor descoperi zero nonconformități critice și mai puțin de 3 nonconformități majore.</p> <p>Acceptarea testelor va fi datată cu ziua când vor fi rectificate toate nonconformitățile descoperite la livrare.</p> <p>Actul de acceptanță a SI SPEG urmează a fi semnat de către Furnizor și STISC.</p>

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Guvernamentală	Clasificare de securitate
		C4 – Public

A2.13. Cerințele procesului de acceptanță a livrabilelor de proiect

Nr.	Categorie cerință	Descriere cerință
1.	Expedierea livrabilelor	Furnizorul trebuie să expedieze livrabilele către persoanele autorizate STISC cu cel puțin 2 zile înainte de data preconizată a semnării acceptanței acestora.
2.	Examinarea livrabilelor	STISC va examina livrabilul recepționat, va prezenta obiecțiile cu referire la sursa obiecției sau va semna livrabilul (în caz de acceptanță a acestuia). Dacă livrabilul este respins sau întors cu obiecții de neconformitate, specialiștii STISC trebuie să identifice problemele sau neconformitățile pentru ca Furnizorul să le abordeze.
3.	Eliminarea și soluționarea neconformităților	Furnizorul este obligat, fără costuri adiționale, să examineze și înlătore neconformitățile recepționate și să remită livrabilul în termen de maxim 5 zile lucrătoare de la recepționarea obiecțiilor. STISC trebuie să accepte, fie să respingă livrabilele retrimise în termen de cinci zile lucrătoare. Livrabilele vor fi considerate acceptate atunci când sunt semnate de către reprezentanții STISC.

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Guvernamentală	Clasificare de securitate
		C4 – Public

Anexa 3. Actele legislative și normative care reglementează procesele de business și procedurile care vor fi automatizate cu ajutorul SI SPEG

Analizând cadrul normativ-legislativ în vigoare al Republicii Moldova și practica internațională pot fi evidențiate un șir de acte, standarde și bune practici, prevederile cărora trebuie luate în considerație la proiectarea, dezvoltarea și implementarea SI SPEG.

În acest sens, pentru dezvoltarea, implementarea și funcționarea SSI SPM a fost identificat un set de 47 acte juridice și normative grupate în funcție de gradul de aplicabilitate după cum urmează:


- cadrul normativ național ce reglementează domeniul utilizării serviciului de poștă electronică în cadrul autorităților publice ale Republicii Moldova;
- cadrul normativ național în domeniul informatizării și tehnologiei informației;
- standarde și bune practici în domeniul TIC.

I. Cadrul normativ național ce reglementează domeniul utilizării serviciului de poștă electronică în cadrul autorităților publice ale Republicii Moldova:

1. Legea nr. 241 din 15.11.2007 privind comunicațiile electronice, Monitorul Oficial nr. 51-54 din 14.03.2008.
2. Hotărârea Guvernului nr. 969 din 23.08.2007 pentru aprobarea Regulamentului privind Sistemul de poștă electronică al autorităților administrației publice, Monitorul Oficial nr. 141-145 din 07.09.2007.
3. Hotărârea Guvernului nr. 546 din 20.07.2011 privind aprobarea Regulamentului cu privire la acordarea serviciilor Sistemului de telecomunicații al autorităților administrației publice și operarea modificărilor în unele hotărâri ale Guvernului, Monitorul Oficial nr. 118-121 din 22.07.2011.
4. Hotărârea Guvernului nr. 822 din 06.11.2012 cu privire la serviciile sistemului de poștă electronică al autorităților administrației publice, Monitorul Oficial nr. 234-236 din 09.11.2012.
5. Hotărârea Guvernului nr. 414 din 08.05.2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat, Monitorul Oficial nr. 157-166 din 18.05.2018.

II. Cadrul normativ național în domeniul informatizării și tehnologiei informației:


6. Legea nr. 982 din 11.05.2000 privind accesul la informație, Monitorul Oficial nr. 88-90 din 28.07.2000;
7. Legea nr. 1069 din 22.06.2000 cu privire la informatică, Monitorul Oficial nr. 73-74 din 05.07.2001.
8. Legea nr. 467 din 21.11.2003 cu privire la informatizare și la resursele informaționale de stat, Monitorul Oficial nr. 6-12 din 01.01.2004;
9. Legea Nr. 71 din 22.03.2007 cu privire la registre, Monitorul Oficial nr. 70-73 din 25.05.2007.
10. Legea nr. 241 din 15.11.2007 a comunicațiilor electronice, Monitorul Oficial nr. 51-54 din 14-03-2008.
11. Legea nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal, Monitorul Oficial nr. 170-175 din 14.10.2011.

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Guvernamentală	Clasificare de securitate
		C4 – Public


12. Legea Nr. 91 din 29.05.2014 cu privire la semnătura electronică și documentul electronic, Monitorul Oficial nr. 174-177 din 04.07.2014.
13. Legea nr. 142 din 19.07.2018 cu privire la schimbul de date și interoperabilitate, Monitorul Oficial nr. 295-308 din 10.08.2018.
14. Hotărârea Guvernului nr. 1123 din 14.12.2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, Monitorul Oficial nr. 254-256 din 24-12-2010.
15. Hotărârea Guvernului nr. 7104 din 20.09.2011 cu privire la aprobarea Programului strategic de modernizare tehnologică a guvernării (e-Transformare), Monitorul Oficial nr. 156-159 din 23.09.2011
16. Hotărârea Guvernului nr. 656 din 05.09.2012 cu privire la aprobarea Programului privind Cadrul de Interoperabilitate, Monitorul Oficial nr. 186-189 din 07.09.2012.
17. Hotărârea Guvernului nr. 1090 din 31.12.2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass), Monitorul Oficial nr. 4-8 din 10.01.2014.
18. Hotărârea Guvernului nr. 128 din 20.02.2014 privind platforma tehnologică guvernamentală comună (MCloud), Monitorul Oficial nr. 47-48 din 25.02.2014.
19. Hotărârea Guvernului nr. 405 din 02.06.2014 privind serviciul electronic guvernamental integrat de semnătură digitală (MSign), Monitorul Oficial nr. 147-151 din 06.06.2014
20. Hotărârea Guvernului nr. 700 din 25.08.2014 cu privire la datele guvernamentale deschise, Monitorul Oficial nr. 256-260 din 29.08.2014.
21. Hotărârea Guvernului nr. 708 din 28.08.2014 privind serviciul electronic guvernamental de jurnalizare (MLog), Monitorul Oficial nr. 261-267 05.09.2014.
22. Hotărârea Guvernului nr. 201 din 28.03.2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică, Monitorul Oficial nr. 109-118 din 07.04.2017.
23. Hotărârea Guvernului nr. 211 din 03.04.2019 privind platforma de interoperabilitate (MConnect), Monitorul Oficial nr. 132-138 din 12.04.2019
24. Hotărârea Guvernului nr. 375 din 10.06.2020 pentru aprobarea Conceptului Sistemului informațional automatizat „Registrul împuternicirilor de reprezentare în baza semnăturii electronice” (MPower) și a Regulamentului privind modul de ținere a Registrului împuternicirilor de reprezentare în baza semnăturii electronice, Monitorul Oficial nr. 153-158 din 26.06.2020.
25. Hotărârea Guvernului nr. 376 din 10.06.2020 pentru aprobarea Conceptului serviciului guvernamental de notificare electronică (MNotify) și a Regulamentului privind modul de funcționare și utilizare a serviciului guvernamental de notificare electronică (MNotify), Monitorul Oficial nr. 149-151 din 19.06.2020.

III. Standarde și bune practici în domeniul TIC:

26. Reglementarea tehnică RT 38370656-002:2006 „Procesele ciclului de viață al software-ului”, aprobată prin ordinul Ministerului Tehnologiei Informației și Comunicațiilor nr.78/2006.
27. Standardul Republicii Moldova SMV ISO CEI 15288: 2009, „Ingineria sistemelor și software-ului. Procesele ciclului de viață al sistemului”.

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Governamentală	Clasificare de securitate
		C4 – Public

28. SM ISO/CEI 12207 „Ingineria sistemelor și software-ului. Procesele ciclului de viață al software-ului”.
29. SM ISO/CEI 14764:2015 - Ingineria software. Procesele ciclului de viață al software-ului. Mentenanță.
30. SM ISO/CEI 27002 „Tehnologia informației. Tehnici de securitate. Cod de bună practică pentru managementul securității informației”.
31. SM ISO/CEI 15408-1 „Tehnologia informației. Tehnici de securitate. Criterii de evaluare pentru securitatea tehnologiei informației. Partea 1: Introducere și model general”.
32. SM ISO/CEI 15408-2 „Tehnologia informației. Tehnici de securitate. Criterii de evaluare pentru securitatea tehnologiei informației. Partea 2: Cerințe funcționale de securitate”.
33. SM ISO/CEI 15408-3 „Tehnologia informației. Tehnici de securitate. Criterii de evaluare pentru securitatea tehnologiei informației. Partea 3: Cerințe de asigurare a securității”.
34. Michael O. Leavitt, Ben Shneiderman, Research-Based Web Design & Usability Guidelines, https://www.usability.gov/sites/default/files/documents/guidelines_book.pdf
35. Recomandările World Wide Web Consortium (W3C) (<http://www.w3c.org>) privind calitatea conținutului paginilor Web, posibilitățile vizualizării corecte a informației, folosind exploratoare Internet larg utilizate, și compatibilitatea cu diferite platforme informatice.
36. Recomandările WAI (Web Accessibility Initiative) (<http://www.w3c.org/WAI>) privind asigurarea posibilității utilizării resurselor site-urilor de către persoanele cu dizabilități.
37. Recomandările WCAG (Web Content Accessibility Guidelines) <http://www.w3.org/TR/WCAG21/>

	Elaborarea Portalului WEB al Sistemului de Poștă Electronică Governamentală	Clasificare de securitate
		C4 – Public

Anexa 4. Calcularea prețului mediu (Pm)

Calcularea prețului mediu

#	Denumirea categoriei expertului	Efort, Om/ore	Cantitatea persoanelor	Total efort, om/ore	Pondere, %	Prețul ofertantului pentru 1 om/oră, fără TVA, lei	Preț mediu, lei
1	2	3	4	5	6	7	8 (6*7)
1.	Business analyst/ Team Leader/ Scrum master	1120	1	1120	11.97%		0.00
2.	Dezvoltator software interfață FrontEnd	1360	2	2720	29.06%		0.00
3.	Dezvoltator software interfață BackEnd	1360	2	2720	29.06%		0.00
4.	Dezvoltator software/ Specialist DevOps	480	1	480	5.13%		0.00
5.	Dezvoltator/ Administrator bază de date	560	1	560	5.98%		0.00
6.	Software Tester și Formator	1120	1	1120	11.97%		0.00
7.	Designer	640	1	640	6.83%		0.00
Suma (Pm)		9360	9	9360	100.00%	-	0.00