SPECIFICAȚII TEHNICE

Destinate dezvoltării platformei digitale

„Avertizori de Integritate”

Extensie funcțională a paginii web oficiale Transparency International Moldova

Chișinău 2025

CUPRINS

1. SCOPUL DOCUMENTULUI

Prezentul document stabilește Termenii de Referință (ToR) pentru elaborarea specificațiilor tehnice necesare dezvoltării și implementării unei **platforme digitale securizate**, destinată facilitării procesului de raportare a practicilor ilegale, faptelor de corupție, abuzurilor sau altor încălcări ale legii, de către avertizorii de integritate.

Platforma va funcționa ca **o extensie integrată a paginii web oficiale a Transparency International Moldova (www.transparency.md)** și va constitui un mecanism digital specializat, ce urmărește consolidarea culturii integrității și protejarea persoanelor care aleg să semnaleze nereguli, în conformitate cu prevederile Legii nr. 122/2018 privind avertizorii de integritate și standardele internaționale relevante în materie de protecție a avertizorilor (*whistleblowers*).

Documentul are scopul de a asigura un cadru clar și detaliat pentru definirea obiectivelor platformei, funcționalităților cheie, cerințelor tehnice și nefuncționale, precum și pentru descrierea condițiilor de interoperabilitate, securitate cibernetică, criptare, anonimizare a datelor și integrare cu infrastructura existentă a organizației. Platforma va permite transmiterea confidențială și, opțional, anonimă a sesizărilor, precum și gestionarea electronică a comunicării între avertizor și personalul autorizat al organizației.

Termenii de Referință servesc drept document de referință pentru toți actorii implicați în procesul de proiectare, dezvoltare, testare și lansare a soluției — inclusiv echipa tehnică, consultanții juridici, experții în protecția datelor și partenerii instituționali. Acest document contribuie la **alinierea așteptărilor între părți, clarificarea responsabilităților și fundamentarea unei abordări strategice coerente și sustenabile** în ceea ce privește digitalizarea canalelor de raportare internă.

Documentul include, de asemenea, reprezentări grafice ale principalelor funcționalități prin intermediul diagramelor de cazuri de utilizare (UML Use Cases), completate de descrieri narative pentru o înțelegere operațională a scenariilor de utilizare. Sunt abordate în mod specific aspecte legate de **asigurarea integrității și confidențialității informației**, utilizarea mijloacelor de autentificare și criptare, precum și compatibilitatea cu politicile organizației privind protecția datelor cu caracter personal.

2. OBIECTIVELE PLATFORMEI

Platforma digitală pentru avertizorii de integritate, dezvoltată ca extensie funcțională a site-ului Transparency International Moldova, urmărește implementarea unui mecanism **intuitiv, securizat și interoperabil**, care să faciliteze raportarea conformă a neregulilor, într-un cadru digital transparent și protejat. Obiectivele principale ale acestei soluții informatice sunt următoarele:

2.1. Asigurarea unui canal digital securizat pentru sesizări

Crearea unei interfețe web criptate end-to-end, prin care avertizorii pot transmite sesizări în mod **anonim sau confidențial**, fără riscul compromiterii identității sau a conținutului raportat. Se va

utiliza un protocol de comunicație **TLS 1.3**, împreună cu mecanisme de **tokenizare** și **pseudonimizare** a datelor personale, pentru a garanta integritatea tranzacțională a informațiilor transmise.

2.2. Digitalizarea procesului de gestionare a sesizărilor

Implementarea unui flux logic automatizat de **preluare, clasificare, analiză și arhivare** a sesizărilor, cu alocarea acestora către personalul specializat, în baza unor **algoritmi de rutare** și **reguli de business configurabile**. Acest sistem va include un **modul de jurnalizare** (audit trail) care va înregistra toate acțiunile relevante, în vederea asigurării trasabilității și a conformității operaționale.

2.3. Crearea unui back-office administrativ dedicat

Dezvoltarea unui **dashboard de administrare** accesibil doar personalului autorizat din cadrul Transparency International Moldova, pentru consultarea, procesarea și arhivarea sesizărilor. Interfața va include funcționalități de **filtrare avansată**, notificări în timp real, **managementul ciclului de viață al sesizării** și generarea de **rapoarte analitice** pe baza datelor centralizate.

2.4. Întărirea cadrului de protecție a avertizorilor

Asigurarea unei **experiențe digitale etice**, în care avertizorul beneficiază de control deplin asupra datelor furnizate, fiind informat în mod transparent despre politicile de confidențialitate, drepturile sale legale și măsurile de protecție implementate. Se va asigura alinierea platformei la cerințele GDPR, precum și la prevederile naționale privind protecția avertizorilor.

2.5. Interoperabilitate și scalabilitate

Proiectarea platformei într-o arhitectură modulară, **scalabilă și containerizată**, compatibilă cu infrastructura web existentă a Transparency International Moldova. Se prevede posibilitatea de **interconectare viitoare cu alte sisteme sau baze de date**, precum registre naționale sau mecanisme internaționale de raportare, folosind API-uri standardizate și metode RESTful.

2.6. Creșterea rezilienței digitale organizaționale

Prin implementarea acestei soluții digitale, organizația va beneficia de o **maturizare a proceselor interne** de recepționare și analiză a semnalărilor, reducând riscurile de eroare umană, **optimizând timpul de reacție** și sporind **capacitatea instituțională de reacție în fața practicilor abuzive**.

3. PUBLIC-ȚINTĂ ȘI ACTORI PRINCIPALI

Platforma digitală este destinată utilizării de către următoarele categorii de actori:

3.1. Avertizori de integritate

Persoane fizice care au luat cunoștință despre fapte de corupție, abuzuri, conflicte de interese, fraude sau alte ilegalități în cadrul instituțiilor publice sau private și doresc să le semnaleze în mod confidențial sau anonim. Utilizatorii vor accesa platforma printr-o interfață web, completând un

formular standardizat și putând atașa **documente, imagini sau alte fișiere digitale** relevante ca probe.

3.2. Administratorii de sesizări (responsabili TI-Moldova)

Personal autorizat din cadrul Transparency International Moldova, care are acces securizat în back-office pentru a analiza, evalua și gestiona sesizările primite. Aceștia vor lucra cu funcționalități avansate de filtrare, etichetare, monitorizare și generare de rapoarte.

3.3. Audit intern și control juridic (rol opțional)

Persoane cu rol limitat de verificare procedurală a modului în care sunt gestionate sesizările, în scopul auditării interne sau asigurării conformității legale.

3.4. Infrastructura web și tehnicieni IT (rol de suport)

Specialiști care asigură mentenanța tehnică, securitatea cibernetică, actualizările de software și asistența în caz de incidente sau disfuncționalități.

4. PRINCIPII DE ARHITECTURĂ TEHNICĂ

Platforma va fi dezvoltată conform unor principii moderne de **arhitectură software modulară, containerizată și scalabilă**, cu accent pe securitate, disponibilitate și performanță. Principalele repere arhitecturale includ:

- **Arhitectură orientată pe microservicii**, cu separarea logică a componentelor (frontend, API, procesare, stocare);
- **Autenticare dual și control granular al accesului** (RBAC – Role Based Access Control);
- **Criptare asimetrică** a fișierelor și datelor sensibile, atât în tranzit (TLS) cât și în repaus (AES-256);
- **Stocare în medii izolate** (sandbox) pentru fișierele încărcate, cu analiză automată de tip anti-malware și limitarea metadatelor;
- **Backup automatizat, failover și logare distribuită**, pentru asigurarea rezilienței platformei;
- **Utilizarea containerelor Docker** și orchestrare prin Kubernetes (acolo unde este aplicabil), pentru gestionarea scalabilă a infrastructurii;
- **Expunerea de API-uri RESTful** securizate, care să permită eventuale integrări viitoare (ex: registre naționale, baze de date, CRM intern etc).

5. FUNCȚIONALITĂȚI ESENȚIALE

Platforma va integra următoarele funcționalități principale:

5.1. Interfață de raportare pentru avertizori

- Formular de sesizare cu **câmpuri dinamice** (tipul încălcării, instituția implicată, data evenimentului, detalii contextuale);
- **Sistem de atașare a fișierelor** (PDF, imagine, audio, video etc.), cu limită de dimensiune și filtru anti-virus;
- Opțiune pentru **transmitere anonimă** sau cu date de contact (nume, e-mail, telefon – opționale);
- Confirmare automată a recepționării sesizării (fără a expune date personale).

5.2. Back-office administrativ

- Dashboard cu vizualizare cronologică a sesizărilor;
- Clasificare tematică și etichetare;
- Mecanisme de filtrare, căutare și atribuire automată;
- Funcționalitate de notare internă și **comentarii între administratori**;
- Export de statistici și rapoarte în format PDF/Excel.

5.3. Jurnal de activitate (audit log)

- Înregistrarea tuturor acțiunilor critice (vizualizare, modificare, descărcare, ștergere);
- Acces doar pentru persoane cu drepturi superioare.

5.4. Sistem de notificări

- Alerte interne pentru sesizări noi;
- Opțional: notificări automate către avertizor, dacă și-a furnizat datele de contact.

6. CERINȚE NEFUNCȚIONALE

Platforma va respecta următoarele cerințe nefuncționale esențiale:

6.1. Securitate

- Criptare end-to-end (TLS 1.3);
- Hashing + salting pentru parole și date sensibile;
- Protecție împotriva atacurilor de tip XSS, CSRF, SQL injection;
- Hosting pe servere conforme ISO/IEC 27001.

6.2. Confidențialitate și conformitate GDPR

- Pseudonimizarea și minimizarea datelor colectate;
- Politici explicite de retenție și ștergere automată a datelor;
- Acces la date doar pe baza principiului *need-to-know*.

6.3. Disponibilitate și performanță

- Timp de răspuns sub 2 secunde pentru 95% din operațiuni;
- Disponibilitate garantată >99,5%;
- Optimizare pentru browsere moderne și dispozitive mobile;
- Accesibil de pe orice tip de browser și dispozitiv.

6.4. Accesibilitate

- Conformitate cu standardele WCAG 2.1 (nivel AA);
- Interfață ușor de utilizat și intuitivă, inclusiv pentru persoane cu dizabilități.

6.5. Extensibilitate

- Posibilitate de adăugare ulterioară a modulelor (ex: chatbot, consiliere juridică, integrare AI);
- Arhitectură containerizată și modulară pentru adaptabilitate la nevoi viitoare.

6.6. Mentenanță și suport

Dezvoltatorul va asigura **mentenanța tehnică corectivă și suportul operațional** al platformei pe o durată de **12 luni calendaristice** de la data lansării oficiale în producție. Suportul va include:

- **Remedierea erorilor software** apărute în timpul exploatării;
- **Optimizarea performanței**, în funcție de necesități și evoluția traficului;
- **Asistență tehnică pentru utilizatori autorizați** (administratori TI-Moldova), în limita unui volum rezonabil de solicitări;
- **Monitorizarea generală a funcționalității platformei** (uptime, loguri, securitate de bază);
- **Instruire tehnică minimă** pentru personalul desemnat.

Totodată, dezvoltatorul este responsabil de:

- **Compilarea completă a codului-sursă și a tuturor artefactelor tehnice**, incluzând fișiere de configurare, scheme de baze de date, documentație tehnică și manuale de utilizare;

- **Instalarea, configurarea și testarea finală a platformei pe infrastructura de hosting** indicată de beneficiar (server propriu sau cloud);
- Asigurarea compatibilității cu mediul de producție și sprijinirea procesului de **transfer al proprietății aplicației și codului sursă**, în conformitate cu termenii contractuali agreați.

7. FLUXUL PROCESULUI

Fluxul operațional al platformei pentru avertizori de integritate este conceput pentru a asigura o **tranziție coerentă, sigură și trasabilă** a fiecărei sesizări de la momentul transmiterii până la închiderea cazului. Acest flux respectă principiile de confidențialitate, integritate a datelor și acces controlat pe roluri.

Etapele procesului:

1. **Accesarea platformei**
    - Avertizorul accesează platforma publică (extensie a site-ului www.transparency.md), secțiunea „Semnalează o neregulă”.
    - Pagina este disponibilă în mod direct, fără autentificare, cu conexiune criptată (HTTPS).
2. **Completarea formularului de sesizare**
    - Avertizorul completează un formular dinamic, care include:
        - Tipul presupusei încălcări;
        - Instituția sau organizația vizată;
        - Descrierea situației;
        - Posibilitatea încărcării de fișiere (documente, imagini, capturi de ecran etc.);
        - Opțional: date de contact (dacă avertizorul dorește să fie informat ulterior);
        - Alegerea nivelului de anonimat.
3. **Transmiterea sesizării**
    - După validarea minimală a câmpurilor obligatorii, sesizarea este transmisă și salvată într-o bază de date securizată.
    - Platforma generează un cod unic de urmărire pentru avertizor (doar dacă acesta a ales o formă de comunicare ulterioară).

4. **Notificarea administratorului**
    - Un administrator autorizat primește notificare internă despre o nouă sesizare, prin sistemul de alertare integrat.
    - Platforma atribuie automat sesizarea către o persoană responsabilă, pe baza criteriilor tematice sau de competență.
5. **Analiza și trierea sesizării**
    - Administratorul analizează conținutul, verifică probele atașate și poate solicita, în mod confidențial, informații suplimentare (dacă avertizorul a furnizat date de contact).
    - Se marchează starea sesizării: „în examinare”, „acceptată spre investigație”, „respinsă – nefundamentată” etc.
6. **Clasificare și raportare**
    - Sesizarea este clasificată tematic și arhivată digital;
    - Se generează rapoarte interne sau publice (cu date anonimizate) privind tipologia cazurilor semnalate, pentru uz instituțional sau comunicare externă.
7. **Închidere și arhivare**
    - După finalizarea procesului, sesizarea este marcată ca „închisă”;
    - Se aplică politica de retenție a datelor (păstrare sau ștergere automată după termenul prevăzut);
    - Dacă este cazul, avertizorul primește un mesaj de confirmare privind finalizarea cazului.

8. CERINȚE PRIVIND CALIFICAREA OFERTANTULUI

La concurs sunt invitate să participe companii care îndeplinesc următoarele condiții:

1. **Specializare și localizare:**
    - ✓ Companiile trebuie să fie **specializate în prestarea serviciilor de dezvoltare software**, cu competențe demonstrabile în acest domeniu;
    - ✓ Să fie **rezidente în Republica Moldova** sau să dispună de **sucursale permanente** pe teritoriul acesteia, care să asigure o prezență operațională activă.
2. **Experiență minimă:**
    - ✓ Companiile trebuie să aibă o experiență de **minim 5 ani** în domeniul dezvoltării software, demonstrată printr-un portofoliu solid de proiecte finalizate.

3. **Experiență relevantă în sectorul public:**

   Se acordă preferință companiilor care au experiență în **elaborarea și implementarea soluțiilor web** pentru **Administrația Publică Centrală (APC)** și **Administrația Publică Locală (APL)**. Acest criteriu asigură cunoașterea nevoilor și specificului activităților în domeniul administrației publice.

4. **Oferta tehnică și de preț:**

   - ✓ Persoanele juridice interesate trebuie să expedieze o **ofertă completă**, care să includă atât o descriere tehnică detaliată a soluției propuse, cât și o ofertă financiară clară și detaliată;
   - ✓ Oferta tehnică trebuie să demonstreze în mod explicit capacitatea companiei de a îndeplini cerințele proiectului, iar cea financiară să fie însoțită de o justificare a costurilor.

5. **Documentație necesară:**

   Companiile ofertante trebuie să prezinte următoarele documente în cadrul ofertei:

   - ✓ **Descriere detaliată a întreprinderii**, incluzând informații despre experiență, resurse umane, capacități manageriale și tehnice;
   - ✓ **Copii ale actelor de înregistrare**, care să confirme statutul juridic al companiei;
   - ✓ **Certificat de lipsă a datoriilor față de buget**, emis de autoritățile relevante;
   - ✓ **Portofoliu de proiecte similare** implementate, care să includă descrieri ale soluțiilor dezvoltate, obiectivele atinse și impactul acestora;
   - ✓ **Referințe de la beneficiarii proiectelor** desfășurate în ultimii 5 ani, care să confirme calitatea serviciilor oferite;
   - ✓ **CV-urile personalului cheie** implicat în proiect, evidențiind calificările și experiența relevantă;
   - ✓ **Descrierea soluțiilor informatice similare** dezvoltate anterior;
   - ✓ **Oferta tehnică detaliată**, estimarea activităților și durata lor, precum și perioadele de garanție și asistență tehnică;
   - ✓ **Oferta financiară detaliată**, care să includă costurile pe etape și componente ale proiectului;
   - ✓ Orice alte documente relevante care pot sprijini evaluarea calificării companiei ofertante.