

# PLANUL DE TESTARE

## Platforma Națională de Voluntariat „voluntar.md”

---

Prezentul Plan de Testare definește strategia, nivelurile, instrumentele și criteriile de calitate pentru asigurarea conformității Platformei Naționale de Voluntariat voluntar.md cu cerințele Caietului de Sarcini. Documentul include cazuri de test pentru fluxurile cheie și o matrice de trasabilitate cerință → test.

## Cuprins

---

Cuprins.....	2
1. Introducere și obiective .....	3
1.1 Scop .....	3
1.2 Domeniu de aplicare .....	3
2. Strategia de testare.....	3
2.1 Tipuri de testare .....	3
3. Medii și date de testare.....	4
4. Criterii de intrare și ieșire .....	4
4.1 Criterii de intrare.....	4
4.2 Criterii de ieșire .....	4
5. Clasificarea și gestionarea defectelor .....	5
6. Cazuri de test.....	5
6.1 Autentificare și autorizare .....	5
6.2 Creare și aprobare program .....	6
6.3 Aplicare voluntar și finalizare.....	6
6.4 Contestații și notificări .....	6
6.5 Public, hartă și multilingv.....	7
6.6 Non-funcțional .....	7
7. Matrice de trasabilitate (cerință → test) .....	7
8. Raportare și livrabile de testare .....	8

## 1. Introducere și obiective

Obiectivul testării este de a valida că platforma voluntar.md îndeplinește integral cerințele funcționale, tehnice, de securitate și de performanță din Caietul de Sarcini, înainte de recepția fiecărui livrabil și a recepției finale.

### 1.1 Scop

- verificarea corectitudinii funcționale a tuturor modulelor (public, voluntar, ONG, minister, admin, transversale);
- validarea conformității cu stack-ul tehnologic și cu cerințele non-funcționale (securitate, performanță, disponibilitate);
- asigurarea acoperirii minime cu teste impuse de TOR (backend  $\geq 80\%$ , frontend  $\geq 70\%$ , endpoint-uri critice, fluxuri E2E);
- furnizarea dovezilor de calitate (rapoarte de test, raport SonarQube) necesare la livrabilul L7.

### 1.2 Domeniu de aplicare

Testarea acoperă toate componentele livrate: API ASP.NET Core, aplicația Angular (inclusiv SSR), baza de date PostgreSQL, integrările și infrastructura (Docker, CI/CD). Sunt excluse din responsabilitatea Prestatorului defecțiunile cauzate de furnizori terți sau de infrastructura beneficiarului, conform clauzelor contractuale.

## 2. Strategia de testare

Strategia urmează modelul piramidei testelor: o bază largă de teste unitare rapide, un nivel intermediar de teste de integrare și un vârf restrâns de teste end-to-end pentru fluxurile critice. Testarea este integrată în pipeline-ul CI/CD și rulată automat la fiecare Pull Request.

Nivel	Instrument	Acoperire minimă (TOR)
Unit (Backend — Application)	xUnit / NUnit	$\geq 80\%$ statement coverage
Integration (API)	WebApplicationFactory + Testcontainers	Toate endpoint-urile critice
Unit (Frontend)	Vitest / Jest	$\geq 70\%$ servicii și componente complexe
End-to-End	Playwright / Cypress	Login, creare program, aprobare program, aplicare voluntar
Performanță	k6 / Lighthouse CI	p95 API; FCP; scor Lighthouse
Securitate	OWASP ZAP / scanare dependențe	Headers, auth, rate limiting, vulnerabilități cunoscute

### 2.1 Tipuri de testare

- **Funcțională** — validarea comportamentului conform cerințelor (CF-01...CF-19).
- **De integrare** — interacțiunea între API, baza de date și componente.
- **End-to-end** — fluxuri complete prin interfața reală.
- **Non-funcțională** — performanță, securitate, disponibilitate, compatibilitate.
- **De regresie** — rulată automat înaintea fiecărui merge pentru a preveni regresările.
- **De acceptanță (UAT)** — realizată de beneficiar pe Staging.

### 3. Medii și date de testare

Testarea folosește mediile definite în arhitectura DevOps:

Mediu	Utilizare în testare
Development	Teste unitare și de integrare rulate local și în CI.
Staging (Pre-Prod)	Teste E2E, testare de performanță, demo și UAT cu conturi demo.
Production	Teste de fum (smoke tests) post-deploy, monitorizare.

Pe Staging sunt configurate conturile demo impuse de TOR (Anexa C a Caietului de Sarcini):

Email	Parolă	Rol
voluntar@demo.md	(configurată de autoritate)	Voluntar
org@demo.md	(configurată de autoritate)	Organizație (ONG)
minister@demo.md	(configurată de autoritate)	Minister
admin@demo.md	(configurată de autoritate)	Administrator

*Datele de test includ seturi reprezentative de programe, oportunități, aplicații și abilități predefinite (Anexa B a TOR), generate prin seeding la inițializarea bazei de date.*

### 4. Criterii de intrare și ieșire

#### 4.1 Criterii de intrare

- cerințele livrabilului sunt aprobate (baseline L1);
- codul este integrat și build-ul CI trece integral (zero warning la Release);
- mediul de testare și datele de test sunt disponibile.

#### 4.2 Criterii de ieșire

- acoperirea minimă cu teste este atinsă (backend ≥ 80%, frontend ≥ 70%);
- toate cazurile de test critice trec (status Pass);
- zero defecte deschise de severitate Critică sau Majoră;
- raportul de analiză statică (SonarQube) nu conține probleme blocante;
- țintele de performanță (p95, Lighthouse) sunt îndeplinite.

## 5. Clasificarea și gestionarea defectelor

Defectele identificate sunt înregistrate în issue tracker, clasificate pe severități (aliniat SLA-ului din TOR) și urmărite până la rezolvare și retestare.

Severitate	Descriere	Timp răspuns	Timp rezolvare
Critic	Platformă inaccesibilă, pierdere date, vulnerabilitate de securitate	2 ore	8 ore
Major	Funcționalitate cheie nefuncțională (login, creare program, dashboard)	4 ore	24 ore
Minor	Erori UI, calcule incorecte fără blocaj, mesaje greșite	8 ore	72 ore
Cosmetic	Îmbunătățiri minore de aspect	La decizia beneficiarului	Planificat

Ciclul de viață al unui defect: *Nou* → *Triat* → *În lucru* → *Rezolvat* → *În retestare* → *Închis* (sau *Redeschis* dacă retestarea eșuează).

## 6. Cazuri de test

Secțiunea prezintă cazurile de test pentru fluxurile cheie. Fiecare caz are un identificator (TC-xx), pași de execuție și rezultatul așteptat. Cazurile marcate sunt automatizate în suita E2E.

### 6.1 Autentificare și autorizare

ID	Caz de test	Pași	Rezultat așteptat
TC-01	Înregistrare voluntar nou	1. Accesează /register. 2. Selectează rol Voluntar. 3. Completează email/parolă valide. 4. Trimite.	Cont creat; redirect către dashboard voluntar; token JWT emis.
TC-02	Login cu credențiale valide	1. Accesează /login. 2. Introdu email+parolă corecte. 3. Trimite.	Autentificare reușită; redirect bazat pe rol; refresh token setat.
TC-03	Login cu parolă greșită	1. Introdu email valid + parolă incorectă. 2. Trimite.	Mesaj de eroare; fără token emis; acces refuzat.
TC-04	Rate limiting la login	1. Trimite > 10 cereri de login/minut de la același IP.	Cererile peste limită sunt respinse (HTTP 429).
TC-05	Acces neautorizat la rută protejată	1. Neautentificat, accesează /admin/dashboard.	Redirecționare la login; acces blocat de guard.
TC-06	Refresh token expirat	1. Cu refresh token expirat, solicită reînnoire.	Reînnoire respinsă; utilizatorul e deconectat.

## 6.2 Creare și aprobare program

ID	Caz de test	Pași	Rezultat așteptat
TC-07	Creare program (stepper 3 pași)	1. Login ONG. 2. Pas 1: info de bază. 3. Pas 2: abilități+activități. 4. Pas 3: confirmă și trimite.	Program creat cu status Submitted; vizibil în coada Ministerului.
TC-08	Validare câmpuri obligatorii	1. În stepper, lasă titlul gol. 2. Încearcă să avansezi.	Avansare blocată; mesaj de validare afișat.
TC-09	Aprobare program (Minister)	1. Login Minister. 2. Deschide program Submitted. 3. Apasă Aprobă.	Status → Approved; notificare trimisă organizației.
TC-10	Respingere cu notă obligatorie	1. Login Minister. 2. Apasă Respinge fără notă.	Acțiune blocată; nota e obligatorie.
TC-11	Solicitare modificări	1. Minister: Solicită modificări cu notă. 2. ONG editează și retrimite.	Status ChangesRequested → Submitted; notă vizibilă organizației.
TC-12	Publicare program aprobat	1. Program Approved. 2. Tranziție la Published.	Program vizibil public în /programs.

## 6.3 Aplicare voluntar și finalizare

ID	Caz de test	Pași	Rezultat așteptat
TC-13	Aplicare la oportunitate	1. Login voluntar. 2. Deschide o oportunitate. 3. Trimite scrisoare motivație + CV.	Aplicare creată cu status pending; notificare către ONG.
TC-14	Acceptare aplicare (ONG)	1. Login ONG. 2. Deschide aplicarea. 3. Acceptă.	Status → accepted; notificare către voluntar.
TC-15	Finalizare program și calcul ore	1. Voluntar: finalizează program cu documente. 2. Confirmă.	Ore calculate automat și adăugate la profil; proiect marcat finalizat.
TC-16	Feedback bidirecțional	1. După finalizare, voluntar și ONG lasă rating+comentariu.	Câte o recenzie/pereche; rating mediu actualizat pe profil.

## 6.4 Contestații și notificări

ID	Caz de test	Pași	Rezultat așteptat
TC-17	Depunere contestație	1. ONG: contestă un program respins cu motiv.	Contestație creată (Submitted); vizibilă Ministerului.
TC-18	Rezolvare contestație	1. Minister: rezolvă contestația cu notă.	Status → Resolved/Rejected; notă transmisă organizației.
TC-19	Notificare în timp real	1. Declanșează un eveniment (ex. aplicare nouă). 2. Verifică clopoțelul.	Badge numeric incrementat; notificare în listă.
TC-20	Marcare notificări ca citite	1. Marchează individual / în masă.	Badge actualizat; istoric păstrat.

## 6.5 Public, hartă și multilingv

ID	Caz de test	Pași	Rezultat așteptat
TC-21	Filtrare reactivă oportunități	1. În /opportunities, aplică filtre (categorie, locație, status).	Lista se actualizează fără reload; paginare corectă.
TC-22	Hartă interactivă (SSR-safe)	1. Încarcă /map. 2. Verifică markeri și popup.	Harta se randează doar în browser, fără erori SSR; markeri funcționali.
TC-23	Comutare limbă	1. Schimbă limba RO→RU→EN din navigare. 2. Reîncarcă pagina.	Toate textele traduse; preferința persistată în localStorage.
TC-24	Statistici agregate în timp real	1. Accesează pagina principală.	Statisticile afișate corespund datelor curente din sistem.

## 6.6 Non-funcțional

ID	Caz de test	Pași	Rezultat așteptat
TC-25	Performanță API (p95)	1. Rulează test de încărcare pe endpoint-uri GET/POST critice.	p95 ≤ 300ms (GET), ≤ 500ms (POST/PUT).
TC-26	Lighthouse	1. Rulează Lighthouse pe paginile cheie (mobile/desktop).	Scor ≥ 80 (mobile), ≥ 90 (desktop); FCP ≤ 2s pe 4G.
TC-27	Headers de securitate	1. Inspectează răspunsul HTTP în producție.	Prezente: CSP, HSTS, X-Frame-Options, X-Content-Type-Options.
TC-28	Audit log imutabil	1. Efectuează o acțiune critică. 2. Încearcă modificarea log-ului.	Acțiunea e înregistrată; log-ul nu poate fi modificat/șters.
TC-29	Backup și restaurare	1. Rulează backup. 2. Restaurează într-un mediu de test.	Restaurare reușită; RPO ≤ 24h, RTO ≤ 4h respectate.
TC-30	Scalare orizontală	1. Rulează 2 instanțe API simultan. 2. Trimite cereri autentificate.	Fără conflict de sesiune; cererile distribuite corect (JWT stateless).

## 7. Matrice de trasabilitate (cerință → test)

Matricea leagă cerințele din Caietul de Sarcini (ID-uri din Matricea de Conformitate) de cazurile de test și de nivelul de testare care le validează. Aceasta asigură că fiecare cerință critică are cel puțin un test asociat.

Cerință (ID)	Descriere scurtă	Cazuri de test / Nivel
CF-01, CF-19	Pagina principală, multilingv	TC-23, TC-24 (E2E, Unit FE)
CF-02, CF-04	Oportunități, hartă	TC-21, TC-22 (E2E, Unit FE)
CF-09, CF-10	Creare/gestionare program (ONG)	TC-07, TC-08, TC-11 (E2E, Integration)
CF-11, CF-12	Aprobare program (Minister)	TC-09, TC-10, TC-11 (E2E, Integration)
CF-07, CF-08	Dashboard voluntar, finalizare	TC-13, TC-15 (E2E, Unit BE)
CF-16	Feedback bidirecțional	TC-16 (Integration, Unit BE)
CF-15	Notificări	TC-19, TC-20 (E2E, Integration)
CF-17	Contestații	TC-17, TC-18 (Integration)

Cerință (ID)	Descriere scurtă	Cazuri de test / Nivel
CF-13	Administrare (utilizatori, organizații)	TC-05 (autorizare) + teste Integration admin
CT-06...CT-12	Backend: API, EF Core, JWT, audit	TC-01...TC-06, TC-28 (Integration, Unit BE)
CT-01...CT-05	Frontend: Angular, SSR, Leaflet	TC-21...TC-23 (E2E, Unit FE)
SE-01, SE-02	Securitate auth, headers	TC-03, TC-04, TC-27 (Integration, Securitate)
SE-04	Audit imutabil	TC-28
PF-01, PF-02	Performanță API, paginare	TC-25, TC-26 (Performanță)
PF-03	Disponibilitate, backup	TC-29
PF-04	Scalare orizontală	TC-30

Cazurile de test detaliate în Secțiunea 6 reprezintă fluxurile cheie obligatorii. Suita completă de teste automatizate (unit, integrare, E2E) este livrată împreună cu codul sursă la livrabilul L7, însoțită de raportul de acoperire și raportul SonarQube.

## 8. Raportare și livrabile de testare

- Raport de acoperire cu teste (backend  $\geq 80\%$ , frontend  $\geq 70\%$ ), generat automat în CI;
- Raport de analiză statică SonarQube (sau echivalent), livrat la L7;
- Raport de execuție a testelor E2E pentru fluxurile cheie;
- Raport de testare de performanță (p95, Lighthouse);
- Proces-Verbal de acceptanță UAT semnat de beneficiar pentru fiecare livrabil.