DALLOL TECH PLC

DeboFund

Crowdfunding and donation platform

Software Requirements Specification (SRS)

Hibir required - Requirements Documentation

Version 1.7.0 | 7 September 2026

Prepared by	Dallol Tech PLC
Product	DeboFund | https://www.debofund.com
Document	Software Requirements Specification (SRS)
Document ID	DFUND-SRS-1.7.0
Standalone pack	DeboFund only - do not combine with other products
Assessment reach	WEB, API
Classification	Confidential - external audit submission. Secrets redacted.
Submitted to	Information Network Security Administration (INSA)
Division	Cyber Security Audit Division, Wollo Sefer, Addis Ababa
INSA contact (from v4.5 form)	Tilahun Ejigu (Ph.D.) | tilahune@insa.gov.et | +251 937 456 374
Portal	Hibir - https://audit.hibir.et

Standards	Web + API + App Hibir guides as applicable to reach | first-phase INSA v4.5 OF/AEAD/001
Readiness statement	READY WITH CONDITIONS
Reviewed by	To be assigned
Approved by	To be assigned

This file is a standalone Hibir technical submission for this product only (SRS, SDD, TDD/LLD, User Guide, or Security). Do not mix it with other Dallol Tech products. It is not an INSA certificate. Trade license and TIN go in administrative slots. Password policy is minimum 8 characters. Test passwords are exchanged on a secure channel.

Document control

Item	Record
Version	1.7.0
Date	7 September 2026
Baseline	Hibir web + API + app guidelines (by reach) + first-phase INSA v4.5 OF/AEAD/001
Hibir mapping	Required: SRS, SDD, TDD/LLD, User Guide. Optional included: Security. Reach-specific API/App checklists when applicable.
INSA mapping	v4.5 OF/AEAD/001 clauses 1 to 8, 4.1 to 4.2.6, and 5.4.1 through 5.4.9 traced in this file
Reach	WEB, API
Product URL	**https://www.debofund.com**

Revision history

Version	Date	Change	Author
1.0.0	46204	Original combined Word packs	Dallol Tech PLC
1.3.0	46251	INSA v4.5 first-phase; independent packs; password min 8	Dallol Tech PLC
1.4.0	46251	Current Hibir web guideline; v4.5 appendix	Dallol Tech PLC
1.7.0	**46272**	**Expanded DFD0/DFD1/ERD; slot-unique content; less cross-file repetition**	**Dallol Tech PLC**

Slot identity

You are reading **01 Requirements Documentation (SRS)** for **DeboFund** (https://www.debofund.com).

Reach for this product: **WEB, API**. Version 1.7.0.

Hibir guidelines: web / API / app as applicable. First-phase / older INSA form: Web Application Security Testing Requirements Document v4.5 (OF/AEAD/001). Still used for legal slots, test-account channel, and API security depth. The current Hibir onboarding checklist is docs.hibir.et.

This file is one independent PDF. Do not merge slots or other Dallol Tech products.

Packaging and rejection rules (stated once in the SRS)

Rule	Compliance
One PDF (or ZIP) per document type	Five separate files for DeboFund
Clear versioned names	Product + slot + v1.7.0
No passwords / private keys in plain text	Secure channel for test accounts

Guidelines: [https://docs.hibir.et/docs/platform/submission_guidelines/web_application_security] (https://docs.hibir.et/docs/platform/submission_guidelines/web_application_security) | API and App guides linked in the assessment-reach section below.

Assessment reach (this product only)

DeboFund is submitted independently. Hibir tracks are selected from the product's real clients:

Reach	Applies?	Guideline
Web application	Required for this product	[https://docs.hibir.et/docs/platform/submission_guidelines/web_application_security] (https://docs.hibir.et/docs/platform/submission_guidelines/web_application_security)
API asset	**Required for this product**	**[https://docs.hibir.et/docs/platform/submission_guidelines/api_security](https://docs.hibir.et/docs/platform/**

submission_guidelines/ api_security)

Documents in this pack cover every applicable reach above. Do not reuse this pack for another Dallol Tech product.

Hibir API Security - SRS checklist (mandatory items)

Source: https://docs.hibir.et/docs/platform/submission_guidelines/api_security

Section	Item	Mandatory	Where
General	API overview and objectives	Yes	Section 1 + API purpose
General	Scope (in/out)	Yes	Section 2
General	Stakeholders (API consumers)	Yes	Section 3
Functional	Functional requirements	Yes	Section 4
Functional	Use cases / API workflows	Yes	Section 6.1
Functional	Acceptance criteria	Yes	Section 6.2
Non-Functional	Performance requirements	Yes	Section 5
Non-Functional	**Security requirements**	**Yes**	**Section 5**

API consumers (DeboFund)

Public campaign reads. Login issues **JWT**. Production must reject placeholder JWT secrets. Webhooks authenticate the **provider**, not a user JWT.

Hibir SRS checklist (mandatory items for this SRS only)

Section	Item	Mandatory	Where in This SRS
General	Project overview and objectives	Yes	Section 1
General	Scope (in/out)	Yes	Section 2
General	Stakeholders	Yes	Section 3
Functional	Functional requirements	Yes	Section 4
Functional	User stories / use cases	Yes	Section 6.1
Functional	Acceptance criteria	Yes	Section 6.2
Non-Functional	**Basic NFRs**	**Yes**	**Section 5**

1. Introduction & Purpose

1.1 Purpose

This Software Requirements Specification (SRS) document provides a comprehensive, formal definition of the functional, non-functional, security, operational, and interface requirements for DeboFund (https://www.debofund.com).

DeboFund is an enterprise-grade crowdfunding and donation platform designed to facilitate public fundraising across medical, emergency, educational, startup, and community categories. It connects individual and institutional donors with verified fundraisers and organizations across Ethiopia and the diaspora.

This document is authored to establish an authoritative technical specification for system development, quality assurance, system verification, and regulatory compliance under the Information Network Security Administration (INSA) Web Application Security Testing Requirements (v4.5 OF/AEAD/001) and the Hibir Security Audit Framework.

1.2 Objectives for This Assessment

- Give INSA a clear map of actors, features, and assets for DeboFund.
- State acceptance criteria that match the deployed system.
- Separate this product from every other Dallol Tech submission.

1.3 Document Scope

The scope of this document encompasses all software artifacts, user interfaces, system APIs, background queues, and data management mechanisms comprising the DeboFund platform v1.7.0 across Web and API channels. Specifically, this SRS covers:

- Public & Donor Interface: Public campaign browsing, donation selection, and hosted payment gateway integration.
- Fundraiser Portal: Campaign submission, recurring donation configurations, fund collection requests, bank account setups, and organizational KYC verification.
- Super Administrator Console: Centralized system control, campaign review, refund batch processing, Salary Giving execution, goods/in-kind donation oversight, sponsor/partner management, queue monitoring, and granular RBAC administration.
- REST API Services: RESTful API endpoints (/api/v1) supporting client authentication, payload exchange, token lifecycle, and secure mobile/external client operations.

1.4 Standalone Packaging & Assessment Reach

In strict adherence to Hibir and INSA audit packaging standards, this document represents an independent, standalone Software Requirements Specification dedicated exclusively to DeboFund. It contains no cross-product dependencies or combined asset packages.

The designated assessment reach for this package comprises:

- WEB Reach: Web Application reach (https://www.debofund.com, /dashboard, /admin)
- API Reach: Application Programming Interface reach (https://www.debofund.com/api/v1)

2. System Overview & Deployment Architecture

2.1 High-Level Architecture & Stack

DeboFund is engineered on a modern, decoupled Model-View-Controller (MVC) architecture with Hierarchical Model-View-Controller (HMVC) module structuring, ensuring strict separation of concerns, scalability, and robust security boundaries.

- Core Application Runtime: PHP 8.2+ executing within a hardened server environment.
- Application Framework: CodeIgniter 4.7.x leveraging modular HMVC routing and secure filtering.
- Database & Storage: Enterprise PostgreSQL relational database with parameterized querying; Redis caching layer recommended for session persistence and API throttling.
- User Interface & Presentation: Responsive Bootstrap 5 framework with server-side rendered views, modular JavaScript, and support for real-time client theme switching (Daylight/Dark mode).
- API Architecture: RESTful JSON API (/api/v1) protected by stateless JSON Web Tokens (JWT) signed using SHA-256 HMAC algorithms.

2.2 Third-Party Service Integrations

The platform interfaces with external transaction, communication, and infrastructure services using encrypted protocols:

- DeboPay Payment Gateway: Native integration featuring HMAC-SHA256 signature verification on webhooks and server-to-server transaction verification APIs.
- Chapa & Telebirr: Direct server-side API verification queries upon client return.
- Stripe Checkout: Hosted checkout session validation enforcing strict server-side state confirmation.
- Direct Bank Transfer: Manual deposit recording subject to mandatory Super Admin verification and ledger posting.
- Notification Providers: Secure SMTP with TLS encryption for system notifications and transactional messaging; SMS gateway integration for multi-factor OTP delivery.

2.3 Hardened Deployment Topology

DeboFund enforces public document root isolation. Web server configurations restrict public execution strictly to the public/ subfolder containing index.php and static assets. Sensitive framework directories (app/, vendor/, writable/, .env) reside completely outside the web-accessible root directory to eliminate code disclosure and unauthorized script execution risks.

Minimum Hosting

Item	Specification
Operating System	Linux
Web Server	Apache, Nginx, or LiteSpeed
Runtime	PHP 8.2+
Database	PostgreSQL 15+
Cache	Redis (optional)
TLS Certificate	Required for production
Document Root	**public/ entrypoint**

3. Stakeholders, Actors & Data Classification

3.1 Platform Stakeholders

Stakeholder	Interest
Dallol Tech PLC	Platform operator, developer, and infrastructure controller
Donors & Supporters	Individuals and corporate entities contributing funds or in-kind goods
Fundraisers & Organizations	Individual creators, non-profit institutions, and community organizations
Super Administrators	Privileged administrative personnel (content moderation, financial oversight, KYC clearance, compliance)
INSA Audit Division	**Technical assessors verifying security architecture against INSA v4.5 guidelines**

3.2 User Roles & Access Boundaries

Actor Role	Access Level &	System Boundaries & Functional Scope

	Interface	
Guest / Public User	Public Portal (Unauthenticated)	Browse active campaigns, categories, success stories, blog posts, submit contact inquiries, initiate guest donations
Registered Donor	Donor Portal / Dashboard	View personal donation history, manage recurring donation profiles, download payment receipts, track in-kind gifts, manage profile settings
Fundraiser / Organiser	Fundraiser Portal (/dashboard)	Create/submit fundraising campaigns, submit KYC verification documents, configure bank accounts, track collected funds, manage recurring donations, access support
Super Administrator	Admin Console (/admin)	Full platform governance: approve campaigns, process refund batches, audit donations, manage Salary Giving and goods, configure CMS/menus, approve KYC, configure integrations, review audit logs
API Client	**REST API (/api/v1)**	**Programmatic machine access via Bearer JWT. Operates within scope-constrained endpoint controls for campaign synchronization and transaction processing**

3.3 User Personas

Persona 1: Abel — Individual Donor

- Age: 35
- Role: Diaspora professional in the United States
- Technical proficiency: Medium
- Daily goal: Support Ethiopian causes from abroad
- Pain points: Finding trustworthy campaigns, paying in USD
- How DeboFund helps: USD support via Stripe, verified campaigns, PDF receipts

Persona 2: Sara — Fundraiser

- Age: 42

- Role: Community organizer raising funds for a medical emergency
- Technical proficiency: Medium
- Daily goal: Reach fundraising goal quickly
- Pain points: Unclear bank transfer processes, donor trust
- How DeboFund helps: KYC verification badge, hosted payments, live donation tracking

Persona 3: Tewodros — Super Administrator

- Age: 35
- Role: Platform administrator at Dallol Tech PLC
- Technical proficiency: Expert
- Daily goal: Approve campaigns, review KYC, process payouts
- Pain points: Fraud prevention, compliance
- How DeboFund helps: KYC review workflow, dual-admin payout approval, immutable audit logs

Persona 4: Hanna — API Partner Developer

- Age: 30
- Role: Integration engineer at a partner accounting firm
- Technical proficiency: Expert
- Daily goal: Sync donation data programmatically
- Pain points: Inconsistent APIs, unclear authentication
- How DeboFund helps: RESTful JSON API, JWT authentication, documented endpoints

3.4 Data Classification Matrix

Data Category	Representative Examples	Sensitivity Level & Security Controls
Authentication Data	BCrypt/Argon2id password hashes, JWT secrets, OTP	HIGH / RESTRICTED. Encrypted at rest, constant-time verification, never exposed

	hashes, active session keys	in client responses or log files
Financial Data	Donation records, transaction refs, payout ledger, bank account details, refund batches	HIGH / CONFIDENTIAL. Server-side verification, strict RBAC isolation, PCI-DSS compliant offsite gateway handling
Personal Data (PII)	Donor names, email addresses, phone numbers, organizational KYC documents, contact entries	MEDIUM / CONFIDENTIAL. Role-scoped access control, input sanitization, minimised exposure on public receipts
Public Content	**Campaign titles, descriptions, category taxonomies, public blog posts, success stories, CMS pages**	**LOW / PUBLIC. Read-accessible across public interface; write operations strictly restricted to authenticated managers/admins**

Applicable Regulations: Ethiopian cybersecurity / INSA web testing. PCI-DSS not claimed (no card PAN stored). GDPR not claimed as a certification.

4. Functional Requirements & Module Specifications

The functional requirements of DeboFund are organized into three primary operational modules: Public & Donor Experience, Super Administrator Governance, and Fundraiser Operations.

4.1 Public & Donor Portal Requirements

Req ID	Functional Requirement	Detailed System Behavior & Verification Criteria
PUB-001	Donate All Campaigns	The system shall render a searchable, filterable catalog of all active public fundraising campaigns upon public request.
PUB-002	Donate Emergency Category	The system shall isolate and display public fundraising campaigns filtered strictly under the Emergency category.
PUB-003	Donate Medical Category	The system shall isolate and display public fundraising campaigns filtered strictly under the Medical donation category.
PUB-004	Donate Education Category	The system shall isolate and display public fundraising campaigns filtered strictly under the Education category.
PUB-005	Donate Startup Category	The system shall isolate and display public fundraising campaigns filtered strictly under the Startup innovation category.
PUB-006	Donate Community Category	The system shall isolate and display public fundraising campaigns filtered strictly under the Community development category.
PUB-007	How to Fundraise Interface	The system shall display structured guidelines, procedural steps, and operational requirements for launching campaigns.

PUB-008	Start a Campaign Navigation	The system shall provide direct public entry points routing users to fundraiser registration and campaign initiation workflows.
PUB-009	Browse Categories Interface	The system shall render a structured taxonomy of all available campaign categories and interest sectors.
PUB-010	About Us Interface	The system shall present organizational backstory, mission statements, regulatory disclosures, and platform governance information.
PUB-011	Success Stories Interface	The system shall display published reports, impact metrics, and completed success stories of fully funded campaigns.
PUB-012	Blog Module	The system shall render published informational articles, updates, news items, and community announcements.
PUB-013	Contact Us Inquiry	The system shall process public contact form submissions, validating input sanitization and routing entries to administrative queues.
PUB-014	Dynamic Currency Changer	The system shall dynamically calculate and re-render campaign target and donation values when users toggle between ETB and USD currencies.
PUB-015	Donate Now Selection	The system shall allow donors to select standard pre-set contribution tiers or enter custom numeric donation amounts for target campaigns.
PUB-016	Donor Profile Entry	The system shall accept optional donor personal detail inputs (Name, Email, Phone) while supporting anonymous contribution flags.
PUB-017	Payment Method Selection	The system shall present supported checkout channels including DeboPay, Chapa, Telebirr, Stripe, and Direct Bank Transfer.
PUB-018	Payment Account Entry	The system shall validate account formats, wallet details, or direct transfer instructions based on the chosen gateway.
PUB-019	Complete Donation Process	The system shall finalize transaction states upon receiving verified server-side payment confirmation and render downloadable digital receipts.
PUB-020	Theme Preference Toggle	The system shall seamlessly render the public interface in either Daylight or Dark visual theme based on user selection.
PUB-021	Language Preference Toggle	The system shall re-render site content and navigation controls in the user's selected operational language.
PUB-022	**Fundraiser Registration**	**The system shall process new user account creation for individual or corporate fundraisers, capturing credential and contact inputs.**

4.2 Super Administrator Governance Requirements

Req ID	Functional Requirement	Detailed System Behavior & Verification Criteria
SUP-001	Central Control Dashboard	The system shall display real-time transaction metrics, pending KYC queues, total funds raised, and platform performance graphs.
SUP-002	Fundraiser Management	The system shall provide comprehensive administration tools to review, activate, suspend, or audit registered fundraiser accounts.
SUP-003	Donation Record Oversight	The system shall maintain a master ledger of all platform donations, supporting multi-criteria filtering, search, and CSV/PDF data export.
SUP-004	Refund Batch Management	The system shall enable authorized admins to structure, review, approve, and execute automated or manual refund batches for canceled campaigns.
SUP-005	Recurring Donation Oversight	The system shall display active subscription profiles, recurring execution schedules, success rates, and donor billing logs.
SUP-006	Payout Management	The system shall allow admins to process, verify, approve, and disburse campaign funds to verified organizer bank accounts.
SUP-007	Salary Giving Administration	The system shall manage corporate payroll deduction partnerships, employee contribution rosters, and recurring payroll allocations.
SUP-008	Goods & In-Kind Management	The system shall track non-monetary physical goods donations, logistics receipts, fulfillment statuses, and donor acknowledgments.
SUP-009	User Account Creation	The system shall enable Super Admins to manually provision administrative, moderator, and operator accounts with defined RBAC roles.
SUP-010	Organization Management	The system shall process legal organizational registrations, institutional profile verifications, and corporate grouping structures.
SUP-011	KYC Submission Review	The system shall present uploaded identity documents, trade licenses, and TIN certificates for admin approval or rejection with feedback.
SUP-012	CMS Menu Management	The system shall allow dynamic creation, reordering, and modification of header, footer, and navigation menus across

		the portal.
SUP-013	CMS Page Management	The system shall provide a rich-text content management engine for drafting, publishing, and editing custom dynamic web pages.
SUP-014	Requirement Setup	The system shall configure statutory campaign requirements, mandatory verification upload criteria, and legal compliance checks.
SUP-015	Sponsor Management	The system shall record, manage, and display corporate sponsor profiles, logos, funding allocations, and matching contribution rules.
SUP-016	Partner Management	The system shall administer institutional partner profiles, cross-promotional linkages, and operational integration parameters.
SUP-017	Reporting Engine	The system shall generate quick-analytics metrics and compile financial and audit PDF/CSV summaries.
SUP-018	Queue Management	The system shall inspect background worker processing statuses and render queue item states.
SUP-019	Bank Account Management	The system shall register and manage platform master settlement accounts and verify fundraiser bank accounts.
SUP-020	Support Center	The system shall manage open platform tickets and route support requests.
SUP-021	System Settings	The system shall update configuration parameters, global preferences, and keys.
SUP-022	DeboPay Integration	The system shall check API connectivity, gateway status, and DeboPay configuration.
SUP-023	Email Service	The system shall dispatch system SMTP transaction email notifications.
SUP-024	Dashboard Widget Customization	The system shall update dashboard layout configuration based on preferences.
SUP-025	Audit Log Monitoring	The system shall record an immutable, timestamped audit trail of all privileged admin actions, login attempts, and data modifications.
SUP-026	Notification Center	The system shall aggregate system alerts, transaction warnings, security flags, and operational dispatches for admin review.
SUP-027	Admin Theme Toggle	The system shall switch the administrative control panel between Daylight and Dark visual interfaces based on preference.

SUP-028	Profile Management	The system shall enable admins to update operational profiles, contact details, and multi-factor authentication methods.
SUP-029	Password Security Management	The system shall process admin password changes, enforcing minimum 8-character length, complexity rules, and old password checks.
SUP-030	**Session Termination (Logout)**	**The system shall securely terminate the administrative session, invalidate active auth tokens, and clear session cookies.**

4.3 Fundraiser Portal Requirements

Req ID	Functional Requirement	Detailed System Behavior & Verification Criteria
FND-001	Fundraiser Control Dashboard	The system shall present personalized metrics on campaign progress, recent contributions, payout statuses, and donor lists.
FND-002	Recurring Donation Tracker	The system shall display active recurring billing profiles established by supporters for the fundraiser's active campaigns.
FND-003	Fund Collection Interface	The system shall provide tools and options to initiate fund withdrawal and payout requests to verified bank accounts.
FND-004	Campaign Submission Engine	The system shall guide fundraisers through multi-step campaign creation, capturing targets, multimedia, categories, and proof documents.
FND-005	Notification Portal	The system shall display real-time updates regarding donation receipts, campaign approvals, KYC updates, and admin messages.
FND-006	Fundraiser Currency Converter	The system shall calculate and render dashboard collection metrics in either ETB or USD currencies based on user selection.
FND-007	Collect Funds Processing	The system shall register fund collection transactions, validating available balances against pending platform fees and holdbacks.
FND-008	KYC Verification Module	The system shall allow fundraisers to upload government IDs, business registration certificates, and TIN records for verification.
FND-	Bank Account	The system shall store and validate bank details (Bank Name,

009	Management	Account Number, IBAN/SWIFT) submitted for payout settlement.
FND-010	Recurring Profile Setup	The system shall enable fundraisers to configure recurring contribution parameters, thresholds, and campaign schedules.
FND-011	My Donations History	The system shall render an itemized history of all incoming contributions received across active and historical campaigns.
FND-012	My Receipts Module	The system shall generate and display official platform transaction receipts for accounting and verification purposes.
FND-013	Salary Giving Portal	The system shall display employer payroll contribution allocations and process organizational salary deduction links.
FND-014	In-Kind Gifts Tracker	The system shall maintain a catalog of physical goods pledged or donated by supporters, tracking logistics status.
FND-015	Notifications Detail	The system shall render detailed notification payload and context upon user selection.
FND-016	Support Center	The system shall allow fundraisers to submit help desk tickets to platform administrators.
FND-017	Profile Management	The system shall allow fundraisers to update personal profile details.
FND-018	Language Preference	The system shall switch portal interface language based on user selection.
FND-019	Theme Preference	The system shall toggle visual theme preference in the portal.
FND-020	Profile Security	The system shall render profile security and account management options.
FND-021	**Logout**	**The system shall invalidate the fundraiser session token and redirect to home.**

4.4 Workflow Descriptions

4.4.1 Campaign Onboarding & KYC Approval Workflow

1. Fundraiser Registration → Public portal (PUB-022)
2. KYC Document Submission → FND-008
3. Regulatory Verification → Super Admin reviews KYC (SUP-011)
4. Campaign Setup → Fundraiser configures bank (FND-009) + campaign (FND-004)
5. Campaign Activation → Super Admin activates campaign for public donations

4.4.2 Public Donation & Payment Gateway Processing Workflow

1. Campaign Selection → Browse categories (PUB-002 to PUB-006), select campaign (PUB-001, PUB-015)
2. Checkout Setup → Amount, currency (PUB-014), optional profile (PUB-016)
3. Payment Gateway Dispatch → Select method (PUB-017, PUB-018)
4. Payment Execution → Hosted gateway validates; campaign progress updates
5. Ledger & Receipting → Confirmation (PUB-019), tax receipt (FND-012), audit ledger (SUP-003, SUP-025)

4.4.3 Fund Collection, Salary Giving & Disbursement Workflow

1. Collection Request → Fundraiser submits payout (FND-003, FND-007)
2. Salary Giving → Corporate employees (FND-013, SUP-007)
3. Audit Verification → Super Admin verifies campaign + bank (SUP-006, SUP-019)
4. Disbursement Execution → Payout batch via bank gateway or DeboPay (SUP-022)
5. Ledger Reconciliation → Financial logs, refund queue (SUP-004), audit records (SUP-025)

5. Non-Functional & Security Requirements

5.1 Password Policy & Identity Management

To prevent credential compromise and brute-force attacks, DeboFund enforces stringent credential controls aligned with INSA v4.5 guidelines:

- Minimum Password Length: All user and administrative passwords created, updated, or reset must be a minimum of 8 characters in length. Where enhanced complexity is configured, passwords must incorporate uppercase letters, lowercase letters, numeric digits, and special symbols.

- Secure Storage: Passwords must never be stored in plain text or reversible encryption. Storage utilizes BCrypt adaptive one-way hashing with dynamic salt generation.
- Account Lockout & Rate Limiting: The platform tracks consecutive failed login attempts, invoking progressive delays and temporary IP lockouts upon exceeding 5 failed attempts within 15 minutes.

5.2 Session Management & Token Security

- Cookie Hardening: Session cookies enforce HttpOnly, Secure (HTTPS only), and SameSite=Lax/Strict flags to eliminate client-side script theft and mitigate CSRF risks.
- API & Webhook Protection: Mobile and external API endpoints utilize stateless Bearer JWTs. Webhooks validate origin authenticity via HMAC-SHA256 signature verification.
- Session Regeneration: Session identifiers are automatically regenerated upon login state changes to prevent session fixation.

5.3 Payment Integrity & Data Handling

- Server-Side Verification: Transaction completion is strictly governed by server-to-server gateway verification. Browser return parameters are never trusted to mark a donation as paid.
- HMAC Validation: All payment gateway webhooks validate payload signatures using shared secret HMAC keys before updating donation or payout statuses.
- Zero PAN Storage: DeboFund does not store, process, or transmit raw credit/debit card PANs or CVVs. All sensitive payment processing occurs on secure gateway pages.

5.4 Performance & Reliability

- Integrity: Paid state only after provider verify; idempotent webhook handling.
- Reliability: Pending donations must not be double-completed on retry.
- Performance: Public campaign pages shall render within 2.0 seconds under normal load.
- Availability: Linux hosting with TLS; database backups are an operations duty.

5.5 Privacy

- Donor PII is minimised.
- Receipts do not include card data.
- No PAN is stored locally.

6. User Stories & Acceptance Criteria

6.1 User Stories

Story ID	As a (Role)	I Want To	So That
US-01	Donor	Pay on a hosted checkout page	My sensitive payment card details never touch or sit on DeboFund servers.
US-02	Fundraiser	Create and publish a fundraising campaign	Supporters can view my story and donate toward a stated monetary goal.
US-03	Super Admin	Review and approve organizer KYC documents	Disbursements and payouts are issued strictly to verified individuals/organizations.
US-04	Donor	Download an official digital receipt	I have documented evidence of my transaction following verified completion.
US-05	Mobile Client	Browse active campaigns via JWT API	The mobile app can securely query platform data without HTML web scraping.
US-06	**INSA Assessor**	**Utilize synthetic donor and admin accounts**	**Security evaluation can be conducted without exposing live donor personal data.**

6.2 Acceptance Criteria

Criteria ID	Criterion Focus	Mandatory System Acceptance Condition
AC-01	Donation Status Transition	A donation transaction shall remain in 'Pending' state until a valid server-to-server provider verification response is received.
AC-02	Browser Return Disregard	A browser return URL callback without corresponding server verification shall never transition a transaction to 'Paid'.

AC-03	Webhook Signature Rejection	Any incoming payment webhook possessing an invalid, missing, or mismatched HMAC signature shall be rejected with HTTP 401/403.
AC-04	Password Enforcement	Any user creation or password reset request providing a password under 8 characters shall be rejected by system validation.
AC-05	Mock Checkout Prevention	Mock payment checkout features shall be hard-disabled and inaccessible whenever CI_ENVIRONMENT is set to 'production'.
AC-06	**PAN Storage Exclusion**	**The database layer shall strictly exclude fields for payment card PANs, CVVs, or expiration dates.**

6.3 Success Metrics (KPIs)

- Completed donations have a provider reference.
- Refunds are operator-initiated, not webhook-invented.
- Public donate path remains usable over HTTPS.
- Zero PAN storage incidents.
- 100% of webhooks pass HMAC verification before state change.
- 100% of payouts to KYC-verified fundraisers only.

7. Testing Scope & Assets Under Test

The testing scope defined in this section outlines the target endpoints, interfaces, and privilege levels submitted for audit under INSA v4.5 OF/AEAD/001 clause 4.2.3.

Asset Name / Function	Target Production URL / Endpoint	Test Account Provisioning & Security Protocol
Public Fundraising Portal	https://www.debofund.com	Publicly accessible. Unauthenticated guest browsing, donation selection, and public content views.

Fundraiser / Donor Dashboard	https://www.debofund.com/dashboard	Provided to INSA Cyber Security Audit Division via secure separate channel. Credentials never stored in dossier.
Admin Console	https://www.debofund.com/admin	Provided to INSA Cyber Security Audit Division via secure separate channel. Full administrative test account.
REST API Endpoint	**https://www.debofund.com/api/v1**	**Provided to INSA Cyber Security Audit Division via secure separate channel. JWT Bearer token authentication.**

7.1 Out-of-Scope Elements

- Payment Provider Internals: Internal banking and authorization infrastructure of external gateways (DeboPay, Chapa, Stripe, Telebirr).
- DeboPay Core Application: DeboPay gateway application logic is submitted under an independent, separate INSA audit dossier.
- Production Data Dumps: Live production donor databases, payment records, and identity files are excluded to maintain privacy compliance.

8. Assumptions & Constraints

8.1 Assumptions

- Production uses TLS 1.2+.
- Local mirrors may use HTTP for engineering only.
- Seeder/demo passwords must be rotated before assessment.
- Trade license and TIN are uploaded in Hibir administrative slots.
- Donors, fundraisers, and admins have reliable internet connectivity.
- Users have modern, standards-compliant web browsers.

- Payment gateways (DeboPay, Chapa, Stripe, Telebirr) remain operational and their APIs stable.
- Test credentials are exchanged via secure channel only.

8.2 Constraints

- The system must run on Linux with PHP 8.2+ and PostgreSQL.
- Ethiopian data residency and INSA regulatory requirements apply.
- Password policy enforces minimum 8 characters.
- Test credentials must be exchanged via secure channel only.
- Readiness for this product: READY WITH CONDITIONS.

9. Data Classification

Type of Data	Examples in DeboFund	Sensitivity
Authentication data	Password hashes, JWT secrets, OTP hashes	High
Personal data	Donor name, email, phone, KYC documents	Medium
Financial data	Donation amounts, payouts, provider refs, refund batches	High
Public content	**Campaign stories, CMS pages, blog posts**	**Low**

Applicable regulations: Ethiopian cybersecurity / INSA web testing. PCI-DSS not claimed (no card PAN stored). GDPR not claimed as a certification.

10. Assets Under Test

Asset	Location
Public Fundraising Portal	https://www.debofund.com
Fundraiser / Donor Dashboard	https://www.debofund.com/dashboard
Admin Console	https://www.debofund.com/admin
REST API	**https://www.debofund.com/api/v1**

Test account credentials are issued on a secure channel only. They are never printed in these five files.

11. INSA 4.1 — Legal and Administrative Documents

These items are mandatory for the Hibir request but are not embedded in the five technical files:

1. Updated trade license (Dallol Tech PLC)
2. TIN certificate
3. System/product patent certificate — submit only if one exists

Upload them in the Hibir administrative slots. Do not place scans of national IDs inside the SRS/SDD/TDD packages.

12. INSA 4.2.2 — Features of the Web Application

This section is the mandatory feature disclosure for Web Application Security Testing Requirements v4.5 section 4.2.2.

12.1 Development Framework

Item	Value
Language	PHP 8.2+
Framework	CodeIgniter 4.7.x (HMVC modules)
Database	PostgreSQL (Redis recommended)
UI	Server-rendered PHP views (Bootstrap admin/public themes)
API style	**REST (JSON)**

12.2 Libraries and Plugins (Application-Level)

Composer: codeigniter4/framework, firebase/php-jwt, predis/predis, endroid/qr-code, dompdf/dompdf, ramsey/uuid.

12.3 Custom-Developed Modules

- Public campaigns and donate wizard
- Fundraiser dashboard, KYC, payouts
- Super admin (campaigns, refunds, Salary Giving, goods donations, CMS)
- Recurring donations
- REST /api/v1 for mobile

12.4 Third-Party Service Integrations

- DeboPay (HMAC webhook + verify API)
- Chapa, Telebirr, Stripe Checkout
- Bank transfer awaiting admin confirmation
- SMTP / SMS OTP

12.5 Actor / User Types

Actor	Interface
Guest donor	Public donate
Registered donor	Dashboard
Fundraiser / organisation	Campaign console
Super admin / moderator	/admin
API client	**JWT /api/v1**

12.6 System Dependencies and Minimum Hosting

Linux, PHP 8.2+, PostgreSQL, Redis optional, TLS. Document root = public/. Mock payments must be off in production.

12.7 Implemented Security Standards or Policies (Design Target)

- INSA Web Application Security Testing Requirements v4.5 (this submission)
- OWASP Top 10 as a testing lens
- TLS 1.2+ for production HTTP
- Role-based access control on privileged functions
- ISO/IEC 27001 is a reference for control themes; this dossier does not claim ISO certification

12.8 Existing Security Infrastructure

CSRF, API throttle, mobile JWT, webhook signatures, password policy (8+ mixed case, digit, special). WAF/IDS hosting-dependent. Default seed credentials must be rotated — listed as a condition.

13. INSA 4.2.3 — Testing Scope

Asset Name	URL / Host	Test Account Credentials
Public fundraising portal	https://www.debofund.com	Provided to INSA Cyber Security Audit Division through a separate secure channel. Passwords, API keys and OTP seeds are not stored in this dossier.
Fundraiser / donor dashboard	https://www.debofund.com/dashboard	Provided to INSA Cyber Security Audit Division through a separate secure channel. Passwords, API keys and OTP seeds are not stored in this dossier.
Admin console	https://www.debofund.com/admin	Provided to INSA Cyber Security Audit Division through a separate secure channel. Passwords, API keys and OTP seeds are not stored in this dossier.

REST API	**https://www.debofund.com/api/v1**	**Provided to INSA Cyber Security Audit Division through a separate secure channel. Passwords, API keys and OTP seeds are not stored in this dossier.**

Test accounts must cover at least guest/public, authenticated user, and administrator privilege levels (INSA 5.4.9). Create dedicated synthetic accounts. Do not use production donor, guest, or patient data.

Out of scope unless INSA issues a separate written expansion:

- Payment-provider internals
- DeboPay's own INSA pack (separate product)
- Production personal donor dumps

14. Password Policy (This Product)

Rule	Value
Minimum length	8 characters
Complexity (where the application enforces it)	Uppercase, lowercase, digit, and special character on create/reset
Storage	Adaptive one-way hash (password_hash / bcrypt or Argon2id). Never store passwords in cookies.
Test accounts	Issued to INSA on a secure channel. Passwords are not printed in any of the five files.
Defaults	**Seeder / README demo passwords must be rotated before testing.**

This policy is implemented in application validation (minimum 8). Older screens that only checked length 6 are being aligned to 8 on privileged paths.

15. Primary Control Flow

Figure: Primary control flow — DeboFund

1. Open the production URL over HTTPS.
2. Authenticate (password minimum 8 characters on create/change).
3. Authorise the requested function.
4. Validate input and persist only authorised fields.
5. Respond over TLS; log security events without secrets.

16. Reconciliation with the July 2026 Word Pack

July Claim	Status
Campaigns, donations, KYC, CMS, DeboPay	Implemented
Recurring / Salary Giving / goods	Present in admin requirements — verify depth live
HTTPS force flag / webhook evidence	Condition — not fully evidenced in the August review
Default seed credentials	Must be rotated before INSA testing
Title as "passed Security Audit"	**Forbidden until an independent test report exists**

17. Compliance Mapping — INSA v4.5

INSA v4.5 Clause	Requirement Description	Hibir Document Slot	Location in Dossier	Status
4.1	Legal & Administrative	Hibir Administrative Slots	Uploaded separately	COMPLIANT
4.2.1	System Architecture	SDD Package (DFUND-SDD-1.7.0)	System Design Document	COMPLIANT
4.2.2	Features & Actors	SRS Package (This Document)	Sections 2, 3, 4	COMPLIANT
4.2.3	Scope & Credentials	SRS Package (This Document)	Section 7	COMPLIANT (Credentials secure)
4.2.4	Security Functions	Security Specification Package	Security Specification Document	COMPLIANT
4.2.5	Coding Standards	Security Specification	Secure Coding Section	COMPLIANT
4.2.6	Prior Reports	Security Specification	Prior Reports Section	COMPLIANT
5.4	**API & Integration**	**TDD / LLD Package**	**Test & Technical Design Document**	**COMPLIANT**

Readiness Statement for Assessment: READY WITH CONDITIONS. Pre-deployment checklist mandates that default seed credentials must be rotated and CI_ENVIRONMENT set to production prior to final INSA evaluation execution.

18. Conclusion

This SRS has been prepared to satisfy the mandatory requirements of the Hibir Web Application Security Service Client Submission Guideline and the INSA Web Application Security Testing Requirements v4.5 (OF/AEAD/001).

It provides a comprehensive, product-specific definition of DeboFund's purpose, scope, stakeholders, functional requirements, non-functional requirements, user stories, acceptance criteria, data classification, testing scope, and compliance mapping.

All mandatory checklist items are addressed:

- ✅ Project overview and objectives
- ✅ Scope (in/out)
- ✅ Stakeholders
- ✅ Functional requirements

- ✅ User stories / use cases
- ✅ Acceptance criteria
- ✅ Basic non-functional requirements

All recommended optional items are also included:

- ✅ User personas
- ✅ Workflow descriptions
- ✅ Advanced non-functional requirements
- ✅ Success metrics (KPIs)
- ✅ Assumptions and constraints