Functional Requirements Document

Customer Account & Engagement Platform

Document Version	1.0
Status	Draft for Review
Prepared By	Business Analysis Team
Date	2026-01-12
Project ID	PR6

Document Control

Revision History

Version	Date	Author	Description of Change
0.1	2026-01-12	B. Analyst	Initial draft
1.0	2026-02-12	B. Analyst	Reviewed and approved for baseline

Approvals

Role	Name	Signature	Date
Product Owner	Noel Assegid		
Engineering Lead	Tabatha Brown		
QA Lead	Carlos Ramirez		

Table of Contents

1. Introduction

1.1 Purpose

This document defines the functional requirements for the Customer Account & Engagement Platform. It describes what the system must do from a user and business perspective, and serves as the basis for design, development, and test planning. Non-functional characteristics (performance, security, availability) are covered in Section 4 at a summary level; detailed non-functional targets are maintained in a separate Non-Functional Requirements Specification.

1.2 Scope

The platform enables end users to register, authenticate, manage their profile, search and export records, and receive notifications, while giving administrators tools to manage accounts, roles, and access. The system also exposes a REST API for third-party integration. This release covers web and mobile-responsive access; native mobile applications are out of scope.

1.3 Intended Audience

- Product and Business stakeholders: to validate that requirements reflect business needs.
- Engineering: to design and implement the system.
- Quality Assurance: to derive test cases and maintain the Requirements Traceability Matrix (RTM).
- Project Management: to plan releases and track scope.

1.4 Definitions, Acronyms, and Abbreviations

Term	Definition
FR	Functional Requirement
2FA	Two-Factor Authentication
RBAC	Role-Based Access Control
SSO	Single Sign-On
GDPR	General Data Protection Regulation
RTM	Requirements Traceability Matrix

1.5 References

- Business Requirements Document (BRD), v1.2
- System Requirements Specification (SRS), v1.0
- Requirements Traceability Matrix (RTM), v1.0
- Compliance Policy: Data Privacy & Retention, v2.0

2. Overall Description

2.1 Product Perspective

The platform is a new, standalone web application that integrates with existing corporate identity, email, and calendar services. It replaces the legacy account portal referenced in the BRD.

2.2 User Classes and Characteristics

User Class	Description
End User	Registers, logs in, manages profile, searches records, receives notifications.
Manager	All End User capabilities plus access to dashboards and reports for their team.
Administrator	Manages user accounts, roles, and system configuration.
External System	Third-party services consuming the REST API under OAuth 2.0.

2.3 Assumptions and Dependencies

- Corporate SSO identity providers (SAML 2.0) will be available in all environments prior to UAT.
- Users have modern browsers (Chrome, Edge, Safari, Firefox: last 2 major versions).
- Email and SMS gateways are provisioned by the infrastructure team ahead of Sprint 4.

3. Functional Requirements

Each requirement below is identified by a unique ID that traces directly to the corresponding entry in the Requirements Traceability Matrix (RTM). Requirements are grouped by functional module.

3.1 Authentication & Access

REQ-001: User Login

Attribute	Detail
Description	The system shall allow users to log in using their registered email address and password.
Priority	High
Trigger	User submits login form with email and password.
Pre-conditions	User has an active, non-locked account.
Processing	System validates credentials against stored (hashed) password; on success, creates an authenticated session; on failure, increments failed-attempt counter.
Post-conditions	User is redirected to their dashboard on success, or shown a generic error message on failure.
Acceptance Criteria	Valid credentials grant access within 2 seconds; invalid credentials are rejected without revealing whether the email or password was incorrect.

REQ-002: Account Lockout

Attribute	Detail
Description	The system shall lock a user account after 5 consecutive failed login attempts.
Priority	High
Trigger	5th consecutive failed login attempt for a given account within 15 minutes.
Pre-conditions	Account exists and is currently unlocked.
Processing	System sets account status to 'Locked', logs the event, and sends a security notification email to the account owner.
Post-conditions	Account is locked for 30 minutes or until unlocked by an administrator.
Acceptance Criteria	On the 5th failed attempt, further login attempts are rejected with a lockout message, even with correct credentials.

REQ-008: Two-Factor Authentication

Attribute	Detail
Description	The system shall support two-factor authentication (2FA) via SMS or an authenticator app.
Priority	High
Trigger	User enables 2FA in account settings, or 2FA is enforced by policy at login.
Pre-conditions	User has a verified phone number or authenticator app registered.
Processing	System generates a time-based one-time code, delivers it via the chosen channel, and validates the code entered by the user before completing login.
Post-conditions	Session is granted only after both password and 2FA code are validated.
Acceptance Criteria	A valid code within its time window succeeds; an expired or incorrect code is rejected and may be retried up to 3 times.

REQ-029: Single Sign-On (SSO)

Attribute	Detail
Description	The system shall support single sign-on via SAML 2.0 for corporate identity providers.
Priority	High
Trigger	User selects 'Sign in with SSO' on the login page.
Pre-conditions	Organization has a configured SAML identity provider integration.
Processing	System redirects to the identity provider, validates the returned SAML assertion, and provisions or matches a local user record.
Post-conditions	User is logged in without entering a platform-specific password.
Acceptance Criteria	A valid SAML assertion results in successful login; an invalid or expired assertion is rejected with an error.

3.2 User Profile Management

REQ-006 : Edit Profile Information

Attribute	Detail
Description	The system shall allow users to update their profile information, including name, phone number, and address.
Priority	Medium
Trigger	User submits the 'Edit Profile' form.
Pre-conditions	User is authenticated.
Processing	System validates input formats (e.g., phone number pattern) and updates the user record.
Post-conditions	Updated profile information is immediately reflected across the platform.
Acceptance Criteria	Valid updates are saved and confirmed; invalid input (e.g., malformed phone number) is rejected with a field-level error.

REQ-014: Upload Profile Picture

Attribute	Detail
Description	The system shall allow users to upload a profile picture in JPG or PNG format, up to 5 MB.
Priority	Low
Trigger	User selects an image file and clicks 'Upload'.
Pre-conditions	User is authenticated.
Processing	System validates file type and size, scans the file for malicious content, resizes it, and stores it.
Post-conditions	The new picture replaces the previous one across the platform.
Acceptance Criteria	Files under 5 MB in JPG/PNG format are accepted; oversized or unsupported files are rejected with a clear error message.

3.3 Search & Reporting

REQ-016: Keyword Search

Attribute	Detail
Description	The system shall allow users to search records using free-text keyword search.
Priority	Medium
Trigger	User enters a search term and submits the search form.
Pre-conditions	User is authenticated and has permission to view the record type being searched.
Processing	System queries the search index and returns matching records ranked by relevance.
Post-conditions	Results are displayed to the user, paginated per REQ-018.
Acceptance Criteria	A search for a known keyword returns the expected record within 1 second for a dataset of up to 1 million records.

REQ-022 : Report Export

Attribute	Detail
Description	The system shall support exporting reports in PDF, Excel, and CSV formats.
Priority	Medium
Trigger	User clicks 'Export' on a report and selects a format.
Pre-conditions	Report has been generated and is displayed on screen.
Processing	System renders the report data into the selected file format and streams it to the browser for download.
Post-conditions	A file download begins in the user's browser.
Acceptance Criteria	Exported files open correctly in the corresponding application and contain the same data shown on screen.

3.4 Integration & API

REQ-036: REST API for Integrations

Attribute	Detail
Description	The system shall provide a REST API enabling third-party systems to read and write core platform data.
Priority	Medium
Trigger	External system sends an HTTP request to a published API endpoint.
Pre-conditions	External system holds a valid OAuth 2.0 access token.
Processing	System authenticates the request, applies rate limiting, validates the payload, and performs the requested operation.
Post-conditions	A JSON response is returned with the result or an appropriate error code.
Acceptance Criteria	Valid, authenticated requests within rate limits succeed; unauthenticated or malformed requests return 401/400 with a descriptive error body.

REQ-038: API Rate Limiting

Attribute	Detail
Description	The system shall rate-limit API requests to 1,000 requests per hour per client.
Priority	Medium
Trigger	A client's cumulative request count within a rolling 1-hour window reaches the configured limit.
Pre-conditions	Client is authenticated with a valid API key or token.
Processing	System tracks per-client request counts and rejects requests exceeding the threshold with HTTP 429.
Post-conditions	Client receives a 429 response with a Retry-After header once the limit is exceeded.
Acceptance Criteria	Clients under the limit are unaffected; clients over the limit consistently receive 429 until the window resets.

3.5 Compliance & Data Privacy

REQ-047: GDPR Data Deletion

Attribute	Detail
Description	The system shall process user data deletion requests in compliance with GDPR, within 30 days of request.
Priority	High
Trigger	User or administrator submits a verified data deletion request.
Pre-conditions	Request is authenticated and identity is verified.
Processing	System anonymizes or deletes personal data across all subsystems, retaining only legally required records, and logs the action.
Post-conditions	User's personal data is no longer retrievable through normal system function.
Acceptance Criteria	Deletion requests are completed and confirmed to the requester within 30 calendar days, with an auditable log of the action.

REQ-049: Cookie Consent

Attribute	Detail
Description	The system shall display a cookie consent banner to users on their first visit.
Priority	Medium
Trigger	User loads the site for the first time in a browser session without a stored consent preference.
Pre-conditions	None.
Processing	System displays a banner allowing the user to accept or customize cookie categories, and stores the resulting preference.
Post-conditions	Non-essential cookies are only set after consent is granted.
Acceptance Criteria	The banner appears on first visit and does not reappear once a preference has been recorded, until the preference expires or is cleared.

3.6 Administration

REQ-012: Role-Based Access Control

Attribute	Detail
Description	The system shall support role-based access control with, at minimum, Admin, Manager, and User roles.
Priority	High
Trigger	A user attempts to access a page, feature, or API endpoint.
Pre-conditions	User is authenticated and has an assigned role.
Processing	System checks the user's role against the permissions required for the requested resource.
Post-conditions	Access is granted or denied based on role permissions.
Acceptance Criteria	Users can access only the features permitted by their assigned role; unauthorized access attempts are blocked and logged.

REQ-010: Deactivate User Account

Attribute	Detail
Description	The system shall allow administrators to deactivate a user account.
Priority	Medium
Trigger	Administrator selects a user and chooses 'Deactivate' in the admin console.
Pre-conditions	Administrator is authenticated with Admin role.
Processing	System sets the account status to 'Inactive', immediately terminates any active sessions, and logs the action with the administrator's identity.
Post-conditions	The user can no longer log in until the account is reactivated.
Acceptance Criteria	A deactivated account is denied login immediately, and the action is visible in the audit log with actor and timestamp.

4. Non-Functional Requirements (Summary)

The following non-functional expectations apply across the functional requirements above. Detailed targets, test methods, and monitoring approach are defined in the Non-Functional Requirements Specification.

Category	Summary Expectation
Performance	Pages load within 2 seconds under normal load; the system supports 10,000 concurrent users.
Security	Data encrypted at rest (AES-256) and in transit (TLS 1.2+); all authentication events are logged.
Availability	99.9% uptime SLA, with daily backups retained for 30 days.
Accessibility	WCAG 2.1 AA conformance across all user-facing screens.
Localization	English, Spanish, and French supported at initial launch.

5. Assumptions and Constraints

- The system will be hosted in the organization's approved cloud environment.
- Third-party integrations (calendar, SMS) are subject to the availability and rate limits of external vendors.
- Legacy data migration from the current portal is addressed in a separate Migration Plan, not in this document.

6. Open Issues

ID	Issue	Owner	Target Date
ISS-01	Confirm SMS gateway vendor for 2FA delivery.	M. Chen	[Date]
ISS-02	Legal review of GDPR deletion workflow pending.	A. Lee	[Date]