Phase 7: Integration & External Access

This phase establishes the current, internal state of the Lost & Found Portal and, more importantly, defines the strategic roadmap for externalizing access and integrating with mission-critical institutional systems. While the Minimum Viable Product (MVP) operates largely within Salesforce, this documentation provides a robust plan for scalability using advanced integration patterns.

Concept	Project Goal
Integration Strategy	Maintain a secure, internal solution for the MVP while architecting the future use of **Experience Cloud** for external user submissions and **Platform Events** for real-time synchronization with campus security systems.

7.1 Current State (Internal Focus)

The initial deployment of the Lost & Found Portal is an internal application focused on maximizing **Security Staff** efficiency.

Concept	Implementation Details	Reason for Absence / Current Status
Web Services (Callouts)	None implemented in the current scope.	The core business process (matching, queue assignment) is handled entirely by internal Salesforce automation (Flows/Apex) and does not require communication with external APIs.
Remote Site Settings	Not required.	Since no Apex HTTP Callouts are executed, no external endpoints needed whitelisting.
API Limits	Low impact.	Current usage relies on internal Salesforce transaction limits (Apex/Flow DML), keeping API consumption minimal.

7.2 Future Scope A: External Access & User Engagement

The primary integration priority is externalizing the reporting process to drive user adoption and self-service.

7.2.1 Experience Cloud Portal (Digital Experience)

- **Goal:** Implement a dedicated **Experience Cloud Portal** (e.g., lostandfound.institution.edu) to allow external users (Students, Staff) to interact directly with the system without logging into the internal CRM.
- **Functionality:**
    1. **Submission:** Users can submit new **Lost Item** and **Found Item** records using custom web forms.
    2. **Self-Service Search:** Users can search existing open **Found Item** records to see if their lost item is already in inventory.
    3. **Status Tracking:** Authenticated users can log in to view the status of their reported **Lost Item** claim.

7.2.2 Authentication & Security

- **OAuth & Authentication:** The portal will use an **OAuth** flow (e.g., standard login or SAML integration) to authenticate users against the institution's existing identity provider (e.g., LDAP or Active Directory), ensuring single sign-on (SSO) is maintained.
- **Guest User Profile:** A secured **Guest User Profile** will be configured to allow anonymous users to view limited **Found Item** details and submit new reports without logging in.

7.3 Future Scope B: System Integration

To maximize the value of the portal, integration with other institutional systems is planned.

7.3.1 Security Ticketing System Integration (REST Callout)

- **Need:** High-value or sensitive lost items (e.g., laptops, access cards) may need immediate escalation to a separate, specialized security ticketing platform (e.g., ServiceNow, JIRA).
- **Method:** A **Named Credential** will be created to securely store the endpoint URL and required authentication parameters (e.g., API Key). An **Apex Callout** will be triggered *after* a **Lost Item** is saved (via a Flow), communicating with the external ticketing API to create an incident.

7.3.2 Platform Events for Real-Time Status

- **Goal:** Provide external systems (e.g., campus mobile app, digital signage) with real-time updates when a high-profile item is found.
- **Method:** A custom **Platform Event** (e.g., Item_Verified_Match__e) will be published whenever a **Verification Case** is closed and marked as a successful match.

External systems can then **subscribe** to this event stream to immediately display notifications.

7.4 Security and Protocol Summary

Protocol	Purpose in Integration
Named Credentials	Essential for securely storing authentication details (username/password or tokens) for future REST Callouts to external security/ticketing systems.
External Services	Can be leveraged to define the schema of external APIs (e.g., the security ticketing API) in a declarative manner, allowing Flow Builder to call them without requiring complex Apex code.
API Limits	Continuous monitoring will be required post-deployment to ensure that high-volume processes (like future event streams or daily bulk reports) do not exceed daily or transactional API consumption limits.