# Org Setup & Security Configuration

## Phase 2 Implementation Documentation

Prepared by: Salesforce Admin Team
Date: September 2025

# Executive Summary

This document provides a detailed breakdown of Phase 2: Org Setup & Security Configuration for the Enrollment object and supporting organizational settings. The setup ensures strong security, structured access management, and reliable data integrity within the Salesforce environment. Key highlights include private OWDs, modular permission sets, and enforcement of validation rules to maintain clean and consistent data. Login policies and role hierarchies provide governance and controlled access, while company information ensures correct localization, time zone, and fiscal year settings.

## Company Information Setup

- Navigated to Setup → Company Information
- Verified and updated:
- - Company Name: EdTech Enrollment Systems
- - Primary Contact: Admin user
- - Default Locale: English (India)
- - Time Zone: Asia/Kolkata
- - Currency: INR (■)
- Set Fiscal Year to standard calendar year (Jan–Dec)
- Configured Business Hours and Holidays for automation logic (e.g., task due dates, escalation rules)

## Custom Object: Enrollment

- Created a custom object named Enrollment to track student applications.
- Key Fields:
- - Student_Name__c (Text): Captures full name of the applicant.
- - Program_Type__c (Picklist): Options like Full-Time, Part-Time.
- - Status__c (Picklist): Tracks application stage—New, Approved, Rejected, Waitlisted.
- - Counselor__c (Lookup to User): Assigns a staff member to the record.
- - Enrollment_Date__c (Date): Stores the date of application.

## Roles & Profiles

- Defined a role hierarchy:
- - Admin: Full access to all records.
- - Counselor: Access to assigned or shared enrollments.
- - Student: Read-only access to their own record (if exposed via Experience Cloud).
- Customized profiles:
- - Controlled tab visibility and field-level security.
- - Restricted access to sensitive fields like Rejection_Reason__c for non-admins.

## Permission Sets

- Created modular permission sets for flexible access control:
- - Enrollment Viewer: Grants read-only access to Enrollment records.
- - Enrollment Editor: Allows create/edit access for counselors.
- Assigned permission sets based on user responsibilities, not just profiles.

## Organization-Wide Defaults (OWD)

- Set OWD for Enrollment to Private to ensure records are only visible to owners and users with explicit access.
- Enabled role hierarchy so managers can see records owned by subordinates.

## Sharing Rules

- Created criteria-based sharing rules:
- - Example: If Program_Type__c = "Full-Time", share with public group Full-Time Counselors.
- Used public groups to simplify sharing logic and scale access control.

## Login Policies

- Configured login hours for Student profile to restrict access outside business hours.
- Set IP ranges for internal users to prevent unauthorized access from unknown networks.

## Validation Rules

- Enforced data integrity with formulas:
- - Prevent status update unless Program_Type__c is selected: ISBLANK(Program_Type__c) && NOT(ISBLANK(Status__c))
- - Block submission if Enrollment_Date__c is in the past.

# Conclusion

The Phase 2 implementation builds a secure and scalable foundation for managing student enrollments. With properly defined roles, profiles, and permission sets, access is tailored to user responsibilities. Data privacy is preserved by restricting sensitive fields, while validation rules guarantee data consistency. The configuration also ensures compliance with governance standards by enforcing login hours, IP restrictions, and company-wide settings such as locale and fiscal year. This framework provides a strong baseline for future enhancements, such as automation flows and Experience Cloud integration.