Phase 9: Security and User Permissions (Library Book Borrowing System)

Goal

To ensure that the Library Book Borrowing System in Salesforce maintains data security, privacy, and proper access control through profiles, permission sets, organization-wide defaults (OWD), and sharing settings.

Step 1: Objective of Security Setup

The purpose of this phase is to:

- Protect sensitive library data.
- Assign appropriate access levels to users based on their roles.
- Ensure that users can perform only those actions permitted by their job responsibilities.

Screenshot: Setup home showing Security section in Salesforce.

Step 2: Define Security Requirements

Objective

Identify who should have access to what data within the Library System.

Access Matrix

Role	Access Level	Objects	Permissions
Library Manager	Full Access	Books, Students, Borrow Records	Create, Read, Edit, Delete
Librarian	Moderate Access	Books, Borrow Records	Create, Read, Edit
Assistant Librarian	Limited Access	Books, Students	Read Only
Student User	Minimal Access	Books	Read Only

Screenshot: Access control table or user role hierarchy.

Step 3: Configure Organization-Wide Defaults (OWD)

Objective

Set baseline record visibility for all objects.

Steps

1. Go to **Setup → Sharing Settings**.
2. Under **Organization-Wide Defaults**, click **Edit**.
3. Set access levels:

- **Book:** Public Read Only
- **Student:** Public Read Only
- **Borrow Record:** Private (only owner and admins can view)

4. Click **Save**.

Expected Result: All users can view Books and Students but see only their own Borrow Records.

Screenshot: OWD configuration screen showing access levels.

Step 4: Create Role Hierarchy

Objective

Establish a hierarchy that allows managers to view subordinate data.

Steps

1. Go to **Setup → Roles → Set Up Roles**.
2. Create the following hierarchy:
   - CEO → **Library Manager** (Top Level)
   - Director → **Librarian** (Reports to Library Manager)
   - Customer Support → **Assistant Librarian** (Reports to Librarian)
3. Assign users to respective roles.

Expected Result: Data automatically rolls up to higher roles in the hierarchy.

Screenshot: Role hierarchy tree structure.

Step 5: Set Up Profiles

Objective

Define permissions that control what users can do within the application.

Steps

1. Go to **Setup → Profiles → Clone an existing profile**.
2. Create the following profiles:
   - **Library Manager Profile** (clone from System Administrator)
   - **Librarian Profile** (clone from Standard User)
   - **Assistant Librarian Profile** (clone from Read Only)
3. Edit each profile's **Object Settings** to configure permissions:
   - **Library Manager:** Full CRUD access on all custom objects.

- **Librarian:** Read/Edit/Create on Book & Borrow Record.
- **Assistant Librarian:** Read-only on Books & Students.

4. Save and assign profiles to users.

Screenshot: Profile setup page showing object permissions.

Step 6: Create Permission Sets (Fine-Tuning Access)

Objective

Grant additional permissions without changing profiles.

Steps

1. Go to **Setup → Permission Sets → New**.
2. Create Permission Sets:
   - **Report Access** – Allows users to run reports and view dashboards.
   - **Data Import Access** – Allows users to use the Data Import Wizard.
3. Under **Object Settings**, enable Read/Write on required objects.
4. Assign permission sets to Librarian and Manager users.

Expected Result: Users gain extra privileges without profile modification.

Screenshot: Permission Set detail page with assigned users.

Step 7: Configure Sharing Rules

Objective

Enable record sharing across roles or specific users when needed.

Steps

1. Go to **Setup → Sharing Settings → Sharing Rules**.
2. Under **Borrow Record Sharing Rules**, click **New**.
3. Define a rule:
   - **Rule Name:** Borrow_Sharing_to_Librarian.
   - **Rule Type:** Based on Record Owner.
   - **Shared With:** Librarian Role.
   - **Access Level:** Read/Write.
4. Save and activate the rule.

Expected Result: Librarians can view and edit borrow records owned by others.

Screenshot: Borrow Record Sharing Rule configuration.

Step 8: Field-Level Security (FLS)

Objective

Restrict visibility of sensitive fields to authorized users only.

Steps

1. Go to **Setup → Object Manager → Student → Fields & Relationships**.
2. Click a sensitive field (e.g., Email or Roll Number).
3. Under **Set Field-Level Security**, uncheck visibility for Assistant Librarian and Student roles.
4. Repeat for any confidential fields (e.g., Contact Number).
5. Save.

Expected Result: Only authorized profiles can see or edit sensitive fields.

Screenshot: Field-Level Security screen for Student object.

Step 9: Login and Session Security

Objective

Add extra layers of security to prevent unauthorized access.

Steps

1. Go to **Setup → Session Settings**.
2. Configure:
   - **Session Timeout:** 30 minutes.
   - **Lock sessions to the domain.**
3. Go to **Setup → Password Policies** and set:
   - **Password Expiration:** 90 days.
   - **Minimum Length:** 8 characters.
4. Enable **Two-Factor Authentication (2FA)** for Manager accounts.

Expected Result: Users experience secure login and controlled sessions.

Screenshot: Password Policy and Session Settings screens.

Step 10: Testing Security Settings

Objective

Verify that access and security configurations work as intended.

Steps

1. Log in as each user (Manager, Librarian, Assistant Librarian).
2. Attempt to:
   - Create or edit records.
   - View reports and dashboards.
   - Access restricted fields.
3. Confirm that:
   - Access matches the role.
   - Unauthorized users are restricted.

Expected Result: Access control and data protection verified successfully.

Screenshot: Access denied message for restricted user.

Step 11: Audit Trail and Monitoring

Objective

Track user activities for accountability.

Steps

1. Go to **Setup → View Setup Audit Trail**.
2. Review configuration changes by date and user.
3. (Optional) Enable **Field History Tracking** for important fields like Book Status or Borrow Date.
4. Generate **Login History Reports** to monitor user access.

Expected Result: Admin can monitor system activity and data changes efficiently.

Screenshot: Setup Audit Trail list.

Step 12: Security Summary Table

Security Feature	Purpose	Status
OWD	Default record access	✅ Configured
Roles	Hierarchical access	✅ Created
Profiles	Object-level control	✅ Implemented
Permission Sets	Additional access	✅ Assigned

Security Feature	Purpose	Status
Sharing Rules	Record-level sharing	✅ Configured
Field-Level Security	Sensitive data protection	✅ Applied
Session & Password Policies	Login protection	✅ Enforced
Audit Trail	Change monitoring	✅ Enabled

Phase 9 Outcome

- Implemented robust security controls for the Library Book Borrowing System.
- Configured profiles, permission sets, and sharing rules for role-based access.
- Protected sensitive data with field-level and session security.
- Validated all user permissions and audit settings to ensure compliance and safety.