Rubrics for Final Project (100 points)

1. Authentication & User Roles – 15 Points

Criteria	**Points**
Working Login & Logout System	5
Proper Password Hashing & Security	4
Correct Role Implementation (Admin & Staff)	4
Unauthorized access properly blocked	2

---

2. Authorization & Access Control – 10 Points

Criteria	**Points**
Role-based route protection (security.yaml / Controller)	4
Proper access denial (403 / redirect)	3
Role checks in controller & templates	3

---

3. Admin Features – 18 Points

Feature	**Points**
Create users/staff	5
Update user/staff	4
Delete user/staff	4
View all data records	3
Admin dashboard (basic totals)	2

---

4. Staff Features – 15 Points

Feature	**Points**
Create records (products, posts, etc.)	6
Edit own records	5
View records	4

Note: Staff must not access admin-only pages

5. CRUD Functionality – 14 Points

Criteria	Points
Create	4
Read	3
Update	4
Delete with confirmation	3

---

6. Validation, Errors & Security – 10 Points

Criteria	Points
Form validation	4
Flash messages	2
CSRF protection	2
No plain-text passwords	2

---

7. Activity Logs System – 8 Points

Criteria	Points
Logs record **Login & Logout**	2
Logs record **Create, Update, Delete actions**	3
Logs save **User, Role, Action, Date/Time**	2
Logs are **viewable by Admin only**	1

- Must use **Doctrine Entity or Event Subscriber**
- Actions recorded:
    - User login
    - Product creation
    - User deletion
    - Record updates

---

8. User Interface & Usability – 7 Points

Criteria	Points
Clean layout & navigation	3
Role-based menu display	2
Mobile readability	2

---

9. Code Quality & Project Structure – 3 Points

Criteria	Points
Clean controller usage	1
Proper entity & repository usage	1
Organized templates & routes	1

TOTAL = 100 POINTS

Category	Points
Authentication & Roles	15
Authorization	10
Admin Features	18
Staff Features	15
CRUD Operations	14
Security & Validation	10
Activity Logs	8
UI & Usability	7
Code Quality	3
TOTAL	**100**

Rubrics for Final Project (100 points)

Category	Points	Actual Points
Authentication & Roles	15	
Authorization	10	
Admin Features	18	
Staff Features	15	
CRUD Operations	14	
Security & Validation	10	
Activity Logs	8	
UI & Usability	7	
Code Quality	3	
TOTAL	**100**	

REQUIRED SYSTEM FUNCTIONS

These functions are **MANDATORY** for a **passing project**.

ADMIN FUNCTIONS

1. Authentication & Account Control

Admin must be able to:

- Login
- Logout
- Change own password
- View own account profile

---

2. Staff Management (CRUD)

Admin must be able to:

- **Create new user accounts**
  - Admin
  - Staff
- **View all user accounts**
  - Username / Email
  - Role
  - Date created
- **Edit user accounts**
  - Change name
  - Change email
  - Change role
  - Reset password
- **Delete user accounts**
  - With confirmation
- **Disable or archive staff accounts** (or statuses of accounts)

---

3. Admin Dashboard

Admin must be able to view:

- Total users
- Total staff
- Total records (products, posts, etc.)
- Recent activities (from logs)

---

4. Full Data Access (System-Wide)

Admin can:

- View ALL records created by staff
- Edit ANY record
- Delete ANY record
- Search & filter records

---

5. Activity Logs (Admin Only Access)

Admin must be able to:

- View all system logs
- Filter logs by:
    - User
    - Action (Create, Update, Delete, Login, Logout)
    - Date
- View log details:
    - Username
    - Role
    - Action performed
    - Affected data
    - Timestamp
- Logs must be **read-only** (Admin cannot modify logs)

---

6. Security & Access Control (Admin Side)

Admin-only routes must be protected by:

- security.yaml role rules
- Controller-level checks
- Twig role-based menu visibility

Staff must NOT access:

- User management
- Activity logs
- Admin dashboard

STAFF FUNCTIONS

---

1. Authentication

Staff must be able to:

- Login
- Logout
- View own profile
- Change own password

---

2. Record Management (CRUD – LIMITED)

Staff must be able to:

- **Create new records**
(e.g. Products, Posts, Students, Orders – depends on your system)

- **View records**

  - Own records
  - Or all shared records (depends on your system)

- **Edit own records only**

  - Cannot edit admin records
  - Cannot edit other staff records

- **Delete own records only**

- With confirmation prompt

---

3. Access Restrictions (VERY IMPORTANT)

Staff must NOT be able to:

- Create staff/admin accounts
- Access activity logs
- Access admin dashboard
- Delete other users
- Change system roles

If staff bypasses a URL manually → system must return:
- 403 Access Denied **OR**
- Redirect to login/dashboard

---

4. ACTIVITY LOGS – REQUIRED EVENTS

These actions MUST be recorded:

- User login
- User logout
- Admin creates a user
- Admin deletes a user
- Staff creates a record
- Staff edits a record
- Staff deletes a record
- Admin updates any record

Each log must store:

Field	**Required**
User ID	-
Username	-
Role	-

Action	-
Target Data	-
Date & Time	-

Example Activity Log Record (One Row in the Database)

Field	Example Value	Meaning
User ID	3	The unique ID of the user who performed the action
Username	admin01	The username of the person who did the action
Role	ROLE_ADMIN	The user's role
Action	DELETE	What action was performed
Target Data	User: staff05 (ID: 9)	The exact record affected
Date & Time	2025-12-06 10:41:25	When the action happened

Another Example (Staff Updates a Product)

Field	Example Value
User ID	7
Username	staff02
Role	ROLE_STAFF
Action	UPDATE
Target Data	Product: Laptop Asus (ID: 14)
Date & Time	2025-12-06 2:18:09 PM