Final Year Project Management System (FYPMS)

Software Requirements Specification

Functional Requirements for External Stakeholders

December 2025

Contents

1 Functional Requirements for Industrial Mentors

1.1 FR 3.5.1 Log in to the System Using Credentials Provided by Placement Cell

1.1.1 Introduction

The purpose of this functional requirement is to allow the industrial mentor to securely log in to the Final Year Project Management System using credentials issued by the placement cell. This login functionality ensures that only authorized industrial mentors can access the system and perform their assigned responsibilities such as reviewing projects, giving feedback, and scheduling meetings.

Inputs

1. Username or Email ID provided by the placement cell
2. Password assigned to the industrial mentor
3. Login request submitted by the industrial mentor through the system login page

Processing

1. The system verifies the entered username or email against the records stored in the database.
2. The entered password is checked using secure authentication methods.
3. The system confirms that the account belongs to an industrial mentor and that the account is active.
4. If the credentials are valid, the system grants access to the industrial mentor dashboard.
5. If invalid credentials are entered, the system displays an appropriate error message.
6. In case of multiple failed attempts, the system may temporarily restrict access for security purposes.

Abnormal Situations

– If the username or password is incorrect, the system displays an error message.

– If the account is inactive or not approved by the placement cell, login access is denied.

– If the system is under maintenance or network issues occur, login may be delayed.

Methods Used

The system uses secure authentication mechanisms and password encryption techniques to verify login credentials and protect user data.

Outputs

1. Successful login redirects the industrial mentor to their dashboard.
2. Unsuccessful login displays clear error or warning messages.

Performance Requirements

– The login process should complete within 2 to 3 seconds under normal conditions.

– The system should handle multiple login requests simultaneously without performance issues.

Design Constraints

– Login must be performed on the existing university server infrastructure.

– Authentication standards defined by the institution must be followed.

Attributes

– **Security:** Login credentials must be protected using encryption.

– **Availability:** The login function should be available during working hours except scheduled maintenance.

– **Maintainability:** Any future changes in authentication policy should not require major system redesign.

1.2 FR 3.5.2 Reset or Change Password

1.2.1 Introduction

This function allows an industrial mentor to securely reset or change their password. It ensures account security and enables password recovery if the mentor forgets their credentials. The system ensures that mentors can update their password while maintaining secure access to the FYP Management System.

Inputs

1. Registered Email ID or Username
2. Old password (for changing password)
3. New password
4. Confirmation of new password

Processing

1. The system verifies the mentor's identity using the provided email or old password.
2. The new password is checked against password policy rules for strength and format.
3. The system compares the new password and confirmation password to ensure they match.
4. If valid, the system encrypts the new password and updates it in the database.
5. A confirmation notification is sent to the mentor once the password has been successfully updated.

Abnormal Situations

– If the old password is incorrect or the email does not match any account, an error message is shown.

– If the new password and confirmation do not match, the system prompts the mentor to retry.

– If the password does not meet strength requirements, the system provides guidance to create a stronger password.

– If the reset link is expired (for email-based reset), access is denied.

Methods Used

– Password encryption and hashing for secure storage.

– Email verification via secure API for password reset links.

– System logs all password changes for accountability.

Outputs

1. Notification confirming that the password has been successfully changed.
2. Error messages in case of invalid input or mismatch.

Performance Requirements

– Password reset or change should be processed within 3 seconds.

– System should handle multiple password reset requests simultaneously without errors.

Design Constraints

– Must comply with university password policies and encryption standards.

– The function should operate on existing servers without additional hardware.

Attributes

– **Security:** Passwords are securely encrypted, and reset links are time-limited and single-use.

– **Availability:** The function is available 95% of the time during working hours, excluding maintenance.

– **Maintainability:** Updates to password policy or reset logic should not require re-designing the system.

1.3 FR 3.5.3 Update Profile Details

1.3.1 Introduction

This function allows an industrial mentor to update their personal and professional information in the FYP Management System. Keeping profile details accurate ensures effective communication and proper assignment of projects and meetings.

Inputs

1. Mentor Name
2. Contact Information (Email, Phone)
3. Department / Organization

4. Profile Picture (optional)
5. Expertise Areas / Skills

Processing

1. Mentor logs into the system and navigates to the profile update section.
2. The system verifies mentor credentials before allowing any edits.
3. Mentor enters updated information in the relevant fields.
4. System validates input formats (e.g., email format, phone number format).
5. Changes are saved to the database, overwriting previous values.
6. Confirmation message is generated and displayed to the mentor.

Abnormal Situations

– If the mentor enters invalid data (e.g., wrong email format), the system shows an error message.

– If the system cannot save changes due to server/database issues, a failure notification is displayed.

– Unauthorized attempts to modify another mentor's profile are denied and logged.

Methods Used

– Role-based access control ensures only the mentor can edit their profile.

– Database transactions to securely save and update profile information.

– Input validation routines for data correctness.

Outputs

1. Notification confirming profile update success.
2. Error messages for invalid data or failed update.

Performance Requirements

– Profile updates should be saved and reflected in the system within 3 seconds.

– Multiple mentors should be able to update their profiles simultaneously without system delays.

Design Constraints

– Must comply with university data handling standards.

– Function must operate on existing servers without additional hardware.

Attributes

– **Security:** Only the mentor can update their own profile; all changes are logged.

– **Availability:** Profile update function should be available during normal working hours.

– **Maintainability:** Adding new profile fields in the future should not require redesigning the system.

1.4 FR 3.5.4 Industrial Mentor – View Assigned Student Projects

1.4.1 Introduction

The main purpose of this function is to allow Industrial Mentors to view all the projects that are specifically assigned to them by the placement cell. This functionality helps mentors keep track of their responsibilities, ensures that they know which student groups they are guiding, and facilitates organized project supervision. The system ensures that only authorized mentors can access their assigned projects, maintaining data confidentiality and integrity.

Inputs

– Mentor Credentials: Login details provided by the placement cell.

– Assigned Project IDs: Unique identifiers of projects allocated to the mentor.

– Student Project Data: Titles, proposals, progress reports, and related documents uploaded by students.

Processing

– Input Validity Checks:

1. Verify mentor login credentials.
2. Ensure that the mentor is assigned to the specific projects.
3. Validate the existence and accessibility of project data.

– Sequence of Operations:

1. Mentor logs into the system using their credentials.
2. System displays a dashboard of all projects assigned to the mentor.
3. Mentor selects a project to view detailed information and documents.
4. System ensures that project details are current and properly formatted.

Abnormal Situations

– If a mentor attempts to view projects not assigned to them, access is denied.

– Missing or corrupted project files trigger notifications for corrective action.

Methods Used

Role-based access control (RBAC) ensures secure access to only authorized project information.

Outputs

– Dashboard listing all assigned student projects.

– Access to project details, including uploaded documents and submission timelines.

– System logs showing mentor access for auditing purposes.

Performance Requirements

– Project lists and details must load within 2–3 seconds for 99% of requests.

Design Constraints

– Must follow university and departmental data access guidelines.

– Should function on existing institutional servers without additional resources.

Attributes

– **Availability:** Function is accessible during working hours, excluding scheduled maintenance.

– **Security:** Only assigned mentors can access their project data.

– **Maintainability:** Dashboard logic and project display can be updated without system redesign.

1.5 FR 3.5.5 Industrial Mentor – Review Project Documents

1.5.1 Introduction

The main purpose of this function is to allow Industrial Mentors to review the documents submitted by students for their assigned projects. This functionality ensures that mentors can assess the progress, quality, and completeness of student work, provide constructive feedback, and verify compliance with academic and industrial standards.

Inputs

– Mentor Credentials: Login details provided by the placement cell.

– Assigned Project IDs: Unique identifiers of projects allocated to the mentor.

– Student Project Documents: Uploaded proposals, progress reports, final reports, and supplementary files.

Processing

– Input Validity Checks:

1. Verify mentor login credentials and role authorization.
2. Confirm that the mentor is assigned to the selected project.
3. Validate the file format and completeness of uploaded documents (e.g., PDF, DOCX).

– Sequence of Operations:

1. Mentor logs into the system.
2. Selects a specific project from their assigned list.
3. Views and examines uploaded documents for completeness, correctness, and quality.
4. Provides feedback comments if necessary.
5. System logs the review activity and timestamps it.

Abnormal Situations

– Unauthorized access to unassigned projects triggers an error message.

– Corrupted or unsupported file formats generate a notification.

– Missing project files prompt an alert to the coordinator.

Methods Used

Role-based access control (RBAC) for secure and authorized access; database transactions to log review actions.

Outputs

– Reviewed project documents accessible on mentor dashboard.

– Notifications confirming document review logged in the system.

– Audit logs of mentor review activities for accountability.

Performance Requirements

– Documents should open and display within 3–4 seconds for 99% of requests.

Design Constraints

– Document review must adhere to university and departmental guidelines.

– Functionality must work with existing servers without extra hardware.

Attributes

– **Availability:** Accessible during working hours except for scheduled maintenance.

– **Security:** Only assigned mentors can access and review documents; all actions are logged.

– **Maintainability:** Document handling logic can be updated without major system redesign.

1.6 FR 3.5.6 Industrial Mentor – Provide Comments on Projects

1.6.1 Introduction

This function allows Industrial Mentors to provide detailed feedback and comments on student projects. The purpose is to guide students, highlight areas of improvement, and ensure the project aligns with academic and industrial standards.

Inputs

– Mentor Credentials: Login information provided by the placement cell.

– Assigned Project IDs: Unique identifiers for the projects assigned to the mentor.

– Student Project Documents: Submitted proposals, progress reports, and other relevant files.

– Feedback/Comments: Mentor's evaluation notes, suggestions, and recommendations.

Processing

– Input Validity Checks:

1. Verify mentor identity and authorization for the project.

2. Ensure feedback/comments follow character limits and formatting rules.
3. Check that comments correspond to the correct project ID.

– Sequence of Operations:

1. Mentor logs into the system.
2. Selects a project from the assigned list.
3. Views the uploaded documents.
4. Adds comments, suggestions, or guidance notes for the project.
5. Saves and submits the comments, which are logged with timestamps.
6. System sends notifications to students, supervisors, and coordinators regarding the new feedback.

Abnormal Situations

– Attempt to comment on unassigned projects triggers an error.

– System rejects comments exceeding allowed length or incorrect format.

– Network issues may temporarily prevent comment submission.

Methods Used

Role-based access control (RBAC), secure database transactions, automated notifications via email or system alerts, audit logging for accountability.

Outputs

– Mentor comments visible to students and supervisors on dashboards.

– Notifications confirming feedback submission.

– Audit logs of mentor feedback actions.

Performance Requirements

– 99% of comments should be submitted and reflected in the system within 3 seconds.

Attributes

– **Security:** Only assigned mentors can provide feedback; all comments are encrypted and logged.

– **Availability:** Accessible during working hours except scheduled maintenance.

– **Maintainability:** Comment submission logic can be updated without system redesign.

1.7 FR 3.5.7 Industrial Mentor – Schedule Meeting with Project Group

1.7.1 Introduction

This function enables Industrial Mentors to schedule meetings with their assigned student project groups. The purpose is to provide guidance, clarify doubts, review progress, and ensure projects align with academic and industrial standards.

Inputs

– Mentor Credentials: Login information provided by the placement cell.

– Assigned Project IDs: Unique identifiers for projects assigned to the mentor.

– Proposed Meeting Dates and Times: Suggested schedule for discussion with the project group.

– Student Availability Data: Optional input to verify suitable meeting times.

Processing

– Input Validity Checks:

1. Verify mentor identity and project assignment.
2. Check that proposed meeting time is within working hours and not in the past.
3. Validate that the selected students belong to the assigned project group.

– Sequence of Operations:

1. Mentor logs into the system.
2. Selects a project from the assigned list.
3. Chooses a suitable date and time for the meeting.
4. Confirms student group availability.
5. Schedules the meeting and stores it in the system database.
6. Sends notifications automatically to students, supervisors, and coordinators.

Abnormal Situations

– Attempt to schedule meetings outside working hours or in the past triggers an error.

– Conflicts with existing schedules result in a warning for rescheduling.

– Network or server issues may delay scheduling notifications.

Methods Used

Role-based access control (RBAC), secure database transactions, automated notification services, audit logging.

Outputs

– Scheduled meetings visible to mentors, students, and supervisors.

– Notifications confirming meeting details sent to all participants.

– Audit logs of scheduled meetings for accountability.

Performance Requirements

– 99% of meeting schedules and notifications should be processed and reflected in the system within 3 seconds.

Attributes

– **Security:** Only assigned mentors can schedule meetings; meeting data is encrypted and logged.

– **Availability:** Accessible during working hours except for scheduled maintenance.

– **Maintainability:** Scheduling logic can be updated without redesigning the system.

1.8 FR 3.5.8 Industrial Mentor – Receive Submission and Meeting Notifications

1.8.1 Introduction

This function allows Industrial Mentors to receive real-time notifications regarding student project submissions and scheduled meetings. The purpose is to ensure that mentors stay updated on project progress, upcoming meetings, and any changes in submission status.

Inputs

– Mentor Credentials: Login information provided by the placement cell.

– Assigned Project IDs: Unique identifiers for projects assigned to the mentor.

– Submission Updates: Notifications triggered when students submit proposals, progress reports, or final project documents.

– Meeting Schedules: Notifications triggered for scheduled meetings, changes, or cancellations.

Processing

– Input Validity Checks:

1. Verify mentor identity and assignment to the relevant project.
2. Ensure the notification is relevant to the assigned project or meeting.
3. Validate timestamp and content of notifications.

– Sequence of Operations:

1. System monitors project submissions and scheduled meetings.
2. When a submission is made or a meeting is scheduled/updated, the system generates a notification.
3. Notifications are sent via email, dashboard alert, or SMS (if configured).
4. Mentors can view notification details and access the relevant project or meeting.

Abnormal Situations

– Missed notifications due to network or server downtime; the system queues notifications for delivery once the connection is restored.

– Unauthorized access attempts trigger error messages and logging.

– Invalid submission or meeting references trigger system warnings.

Methods Used

Role-based access control (RBAC), secure notification services, database logging, audit trails.

Outputs

– Real-time notifications displayed on the mentor dashboard.

– Email/SMS alerts for submissions and meetings.

– Audit logs showing all notifications sent and received.

Performance Requirements

– 99% of notifications should be delivered and displayed within 3 seconds under normal operating conditions.

Attributes

– **Availability:** Notifications should be accessible 24/7 through the system dashboard, except during scheduled maintenance.

– **Security:** Notifications are restricted to assigned mentors; sensitive content is encrypted.

– **Maintainability:** Notification templates and delivery methods can be updated without redesigning the system.

2 Functional Requirements for Placement Cell Staff

2.1 FR 3.6.1 Log in to the system using university credentials

2.1.1 Introduction

The purpose of this function is to allow authorized staff to securely access the FYP Management System using university-provided credentials. This ensures that only personnel with proper access can monitor projects, track mentor engagement, and view project progress. Secure login maintains data confidentiality and integrity.

Inputs

– University Credentials: Staff must enter their assigned username and password.

– Login Request: Submitted via web interface.

Processing

– **Input Validity Checks:**

1. Verify that credentials match the stored database records.
2. Ensure the account is active and authorized for system access.
3. Check for invalid input formats (e.g., empty fields).

– **Sequence of Operations:**

1. Staff navigates to the login page.
2. Enter username and password and submit.
3. System validates credentials.
4. On success, the user is directed to their dashboard.
5. On failure, an error message is displayed and audit logs are updated.

Abnormal Situations

1. Incorrect username or password triggers error notification.
2. Multiple failed attempts may temporarily lock the account.
3. Network issues may prevent login.

Parameters Affected

– User session status.

– Login timestamps in audit logs.

Degrade Operation

System maintenance or low network bandwidth may delay login.

Methods Used

1. Role-Based Access Control (RBAC) ensures only authorized users access system features.

2. Secure authentication protocols (HTTPS, password hashing).

Outputs

– Access to user dashboard upon successful login.

– Error messages for invalid credentials or failed login attempts.

– Audit logs recording login activity.

Performance Requirements

– **Static Requirement:** System shall allow authorized staff to log in using university credentials.

– **Dynamic Requirement:** 99% of login requests shall be processed within 2 seconds under normal conditions.

Design Constraints

– **Standards Compliance:** Follow university IT security and authentication policies.

– **Hardware Limitation:** Must operate on existing university servers without additional hardware.

Attributes

– **Availability:** Accessible 99% of working hours except planned maintenance.

– **Security:** Encrypted credentials and secure authentication protocols.

– **Maintainability:** Login procedures can be updated without redesign.

– **Transferability / Conversion:** Can integrate with future university authentication systems.

2.2 FR 3.6.2 Reset or Change Password

2.2.1 Introduction

This function allows users to securely reset or change their password in the FYP Management System. It ensures that users can recover access if they forget their credentials and maintain account security by updating passwords regularly.

Inputs

– User Email or Username: The email or username associated with the account.

– New Password: User-provided password that meets the system's security requirements.

– Confirmation Password: User must re-enter the new password to prevent mistakes.

Processing

– **Input Validity Checks:**

1. Verify that the user account exists and is active.
2. Confirm that the new password matches the confirmation password.

3. Check password strength according to security rules (minimum length, special characters, etc.).

– **Sequence of Operations:**

1. User requests a password reset or chooses to change the password.
2. System sends a secure link via email to reset the password (for reset requests).
3. User enters the new password and confirms it.
4. System encrypts the password using secure hashing and updates the database.
5. Confirmation notification is sent to the user about the successful password change.

Abnormal Situations

1. Mismatched new and confirmation passwords trigger an error message.
2. Weak passwords not meeting security requirements are rejected with guidance.
3. Expired reset links prevent unauthorized password changes.

Parameters Affected

– User credentials stored in the database.

– Password change timestamp logged in the system.

Degrade Operation

Low network availability or server maintenance may delay password reset or update notifications.

Methods Used

1. Password hashing to securely store new credentials.
2. Temporary secure email links for password resets.
3. Audit logging for accountability of password changes.

Outputs

– Confirmation message displayed for successful password change.

– Error messages for mismatched passwords, expired links, or invalid inputs.

– Audit log entries recording password reset or change activity.

Performance Requirements

– **Static Requirement:** The system shall allow users to securely reset or change their password at any time.

– **Dynamic Requirement:** 99% of password change or reset requests should be processed within 3 seconds under normal conditions.

Design Constraints

– **Standards Compliance:** Must follow university and industry-standard password security policies.

– **Hardware Limitation:** Password reset/change functions must operate on existing servers without additional hardware.

Attributes

– **Availability:** Available 95% of the time during working hours, except during planned maintenance.

– **Security:** Passwords are encrypted; reset links are single-use and time-limited.

– **Maintainability:** Password management processes can be updated without redesigning the system.

– **Transferability / Conversion:** Future integration with external university authentication systems is supported.

2.3 FR 3.6.3 View Industry-Based Projects

2.3.1 Introduction

This function allows Placement Cell staff to view all industry-based projects registered in the FYP Management System. It ensures proper monitoring of student engagement with industrial partners, tracks mentor assignments, and facilitates oversight of project progress.

Inputs

– User Credentials: Login information for authorized Placement Cell staff.

– Project Filters (Optional): Criteria to search or sort projects, such as project status, student group, or assigned mentor.

Processing

– **Input Validity Checks:**

1. Verify Placement Cell staff login credentials.
2. Ensure staff has access permissions for industry-based projects.
3. Validate filter parameters if applied.

– **Sequence of Operations:**

1. Staff logs into the system.
2. Accesses the list of all industry-based projects.
3. Views project details, including student group, assigned mentor, and project progress.
4. System retrieves real-time data from the database and displays it on the dashboard.

Abnormal Situations

1. Unauthorized access attempts trigger an error message and are logged.
2. Missing project data or mentor assignment records generate a warning notification.
3. System failure or network issues temporarily prevent access, with proper error handling.

Parameters Affected

– Project records accessed by Placement Cell staff.

– Dashboard view logs and audit trails for monitoring access.

Degrade Operation

Heavy server load may slow retrieval of project lists temporarily, but access remains functional.

Methods Used

1. Role-Based Access Control (RBAC) to ensure only authorized staff can view projects.
2. Database queries for retrieving up-to-date project data.
3. Audit logging to record all access for accountability.

Outputs

– List of industry-based projects displayed on the dashboard.

– Project details including student group, mentor, status, and progress.

– Notifications or warnings in case of missing data or access issues.

Performance Requirements

– **Static Requirement:** System shall allow Placement Cell staff to view all industry-based projects securely.

– **Dynamic Requirement:** 99% of project list retrieval requests should be processed within 3 seconds under normal load.

Design Constraints

– **Standards Compliance:** Must follow university guidelines for data access and confidentiality.

– **Hardware Limitation:** Function must operate on existing servers without additional hardware.

Attributes

– **Availability:** Available during working hours; occasional maintenance may cause temporary downtime.

– **Security:** Access restricted to authorized Placement Cell staff; sensitive data is encrypted.

– **Maintainability:** Project viewing logic can be updated without redesigning the system.

– **Transferability / Conversion:** Can integrate with university project management systems in the future.

2.4 FR 3.6.4 View Engaged Industrial Mentor Records

2.4.1 Introduction

This function allows Placement Cell staff to access records of all Industrial Mentors engaged with student projects. It ensures proper monitoring of mentor participation, helps track mentor assignments, and facilitates coordination between students, supervisors, and mentors.

Inputs

– User Credentials: Login information for authorized Placement Cell staff.

– Mentor Filters (Optional): Search parameters such as mentor name, assigned project, or availability status.

Processing

– **Input Validity Checks:**

1. Verify Placement Cell staff login credentials.
2. Ensure staff has authorization to view mentor records.
3. Validate filter or search criteria if applied.

– **Sequence of Operations:**

1. Staff logs into the system.
2. Accesses the section for Industrial Mentor records.
3. Views the list of engaged mentors along with project assignments and contact details.
4. System retrieves real-time mentor information from the database and displays it accurately.

Abnormal Situations

1. Unauthorized access triggers an error message and is logged for security.
2. Missing or incomplete mentor assignment data generates a warning notification.
3. Network interruptions temporarily prevent access, with proper error messages.

Parameters Affected

– Mentor assignment records and project engagement logs accessed by staff.

– Audit logs tracking access and retrieval activity.

Degrade Operation

High server load may slow retrieval of mentor records but access remains functional.

Methods Used

1. Role-Based Access Control (RBAC) ensures only authorized Placement Cell staff can view mentor data.

2. Database queries for retrieving accurate mentor assignment records.
3. Audit logging to track access and maintain accountability.

Outputs

– Complete list of Industrial Mentors engaged in student projects.
– Details of mentor assignments, contact information, and project involvement.
– Notifications or warnings in case of missing or inconsistent mentor data.

Performance Requirements

– **Static Requirement:** The system shall allow Placement Cell staff to view engaged Industrial Mentor records securely.
– **Dynamic Requirement:** 99% of mentor record retrieval requests should be completed within 3 seconds under normal load.

Design Constraints

– **Standards Compliance:** Must follow university guidelines for mentor data confidentiality and reporting.
– **Hardware Limitation:** Function must operate efficiently on existing servers without additional hardware.

Attributes

– **Availability:** Available during working hours, with minimal downtime for maintenance.
– **Security:** Access restricted to authorized staff; mentor records are encrypted.
– **Maintainability:** Mentor viewing functionality can be updated without system redesign.
– **Transferability / Conversion:** Can integrate with university project management systems in the future.

2.5 FR 3.6.7 Track Groups Who Work on Industrial Projects

2.5.1 Introduction

This function allows Placement Cell staff to monitor and track student groups involved in industry-linked projects. It ensures that student progress is aligned with project milestones, facilitates coordination with Industrial Mentors, and provides oversight for timely completion of projects.

Inputs

– User Credentials: Login details for authorized Placement Cell staff.
– Project Identifiers: Unique IDs of industry-linked projects to filter student groups.
– Tracking Filters (Optional): Parameters such as student group name, project stage, or mentor assigned.

Processing

– **Input Validity Checks:**

1. Verify staff login credentials and authorization.
2. Ensure selected project IDs exist and are linked to industry-based projects.
3. Validate any applied filters or search parameters.

– **Sequence of Operations:**

1. Staff logs into the system.
2. Navigates to the student project tracking section.
3. Selects the projects or groups to track.
4. Views real-time progress, submissions, and milestone completion status.
5. System updates tracking logs and timestamps automatically.

Abnormal Situations

1. Unauthorized access attempts trigger an error and are logged.
2. Missing project or group data generates a warning notification.
3. Network interruptions may delay tracking information but system provides proper error messages.

Parameters Affected

– Student group progress records and milestone logs.

– Mentor assignment and tracking data.

– Audit logs for tracking activity.

Degrade Operation

System may experience slower response under high load but remains accessible for tracking purposes.

Methods Used

1. Role-Based Access Control (RBAC) ensures only authorized Placement Cell staff can access student group data.
2. Database transactions to retrieve and update project tracking data reliably.
3. Audit logging to maintain accountability and trace all tracking activities.

Outputs

– Complete list of student groups working on industry-linked projects.

– Current project status, milestones achieved, and mentor assignments.

– Notifications or warnings if data is incomplete or inconsistent.

Performance Requirements

– **Static Requirement:** The system shall allow Placement Cell staff to track student groups on industrial projects securely and efficiently.

– **Dynamic Requirement:** 99% of tracking requests should be processed within 3–5 seconds under normal conditions.

Design Constraints

– **Standards Compliance:** Must follow university policies for student data access and confidentiality.

– **Hardware Limitation:** Function must operate using existing servers without additional hardware requirements.

Attributes

– **Availability:** Accessible during working hours with minimal downtime.

– **Security:** Only authorized staff can view tracking data; all records are encrypted.

– **Maintainability:** Tracking functionality can be updated without major redesign.

– **Transferability / Conversion:** Can integrate with future project management or evaluation modules.

3 Functional Requirements for External Evaluators

3.1 Requirement 1: Log in to the System Using Credentials Provided by the University

3.1.1 Introduction

The purpose of this function is to allow External Evaluators to securely access the Final Year Project Management System (FYPMS) using the credentials provided by the university. This functionality ensures that only authorized evaluators can view, assess, and provide feedback on assigned projects. The system maintains security and access control while facilitating smooth access to project data for evaluations.

Inputs

– Evaluator Credentials: Username and password assigned by the university.

– Authentication Requests: Login attempts submitted via the login interface.

Processing

Input Validity Checks:

1. System verifies the evaluator's username and password.
2. Checks if the evaluator account is active and authorized for project access.

Sequence of Operations:

1. Evaluator enters credentials and submits the login form.
2. System validates credentials and confirms access rights.
3. Upon successful authentication, evaluator is redirected to their dashboard showing assigned projects and notifications.

Abnormal Situations:

1. Incorrect username or password triggers an error message.
2. Inactive or unauthorized accounts are denied access with a notification.
3. Multiple failed login attempts trigger temporary account lock for security.

Parameters Affected:

Login timestamps, session records, and access logs.

Degrade Operation:

Low network bandwidth may slightly delay login response.

Methods Used:

Role-based access control (RBAC) ensures only assigned evaluators access relevant projects.

Outputs

– Successful login redirects the evaluator to their dashboard.

– Failure messages for incorrect credentials, inactive accounts, or unauthorized access.

Performance Requirements

Static: The system shall allow all authorized evaluators to log in securely.

Dynamic: 99% of login requests shall be processed within 2 seconds.

Design Constraints

Standards Compliance: Follows university authentication and security policies.

Hardware Limitation: Login process operates on existing servers without additional resources.

Attributes

Availability: Login functionality should be available 99% of the time.

Security: Credentials are encrypted; system enforces temporary account lock for repeated failed attempts.

Maintainability: Authentication logic can be updated without system redesign.

Transferability/Conversion: Can integrate with future university authentication systems.

3.2 Requirement 2: Reset or Change Password (Time-Limited Access)

3.2.1 Introduction

This function allows External Evaluators to reset or change their account passwords securely. It ensures account security and enables evaluators to regain access in case of forgotten credentials. The system provides a time-limited link for resetting the password to prevent unauthorized access and maintains audit logs of the change.

Inputs

– Email Address: University-registered email for sending the password reset link.

– New Password: Password entered by the evaluator after accessing the reset link.

– Confirmation Password: Re-entry of the new password to confirm accuracy.

Processing

Input Validity Checks:

1. System verifies that the email is registered with the university.
2. Checks that the new password matches the confirmation password.
3. Validates password strength according to university security guidelines.

Sequence of Operations:

1. Evaluator requests password reset via the login interface.
2. System generates a secure, time-limited reset link and sends it to the registered email.

3. Evaluator clicks the link, enters a new password, and confirms it.
4. System hashes and securely stores the new password in the database.
5. A notification is sent confirming successful password update.

Abnormal Situations:

1. Mismatched password and confirmation triggers an error message.
2. Expired reset link prevents password update and prompts a new request.
3. Password not meeting strength requirements triggers an error message.

Parameters Affected:

Evaluator credentials, password change timestamp, and audit logs.

Degrade Operation:

Low network connectivity may delay email delivery or password update processing.

Methods Used:

Cryptography for password hashing, time-limited token generation for secure reset, and email API for notification.

Outputs

– Confirmation of successful password change.

– Error messages for expired links, password mismatch, or weak passwords.

Performance Requirements

Static: System shall allow authorized evaluators to securely reset or change passwords.

Dynamic: 99% of password reset requests shall be completed within 3 seconds under normal conditions.

Design Constraints

Standards Compliance: Must follow university IT security policies and international password handling standards.

Hardware Limitation: Reset process operates on existing servers without additional resources.

Attributes

Availability: Password reset functionality should be available 95% of the time during working hours.

Security: Reset links are single-use and time-limited; new passwords are securely hashed.

Maintainability: Password reset logic can be updated without redesigning the system.

Transferability/Conversion: Can integrate with future university authentication and SSO systems.

3.3 Requirement 3: View Assigned Projects for Evaluation

3.3.1 Introduction

This function allows External Evaluators to view the list of Final Year Projects assigned to them for assessment. It ensures that evaluators have access only to projects they are authorized to evaluate, supporting impartial and organized evaluation processes. The system provides secure access to project details and related documents.

Inputs

– Evaluator ID: Credentials provided by the university to identify the evaluator.

– Assigned Project List: System-generated list of projects allocated to the evaluator.

Processing

Input Validity Checks:

1. System verifies evaluator login credentials and role authorization.
2. Confirms that projects listed are specifically assigned to the logged-in evaluator.

Sequence of Operations:

1. Evaluator logs into the FYPMS using university-provided credentials.
2. System retrieves the assigned project list from the database.
3. Evaluator selects a project to view its details and related documents.

Abnormal Situations:

1. Attempt to access projects not assigned to the evaluator triggers an access denied error.
2. Missing or corrupted project data triggers a warning message.

Parameters Affected:

Access logs, timestamps, and project view history.

Degrade Operation:

Temporary network issues may delay retrieval of assigned projects.

Methods Used:

Role-based access control (RBAC) and secure database queries.

Outputs

– Display of assigned projects with project ID, title, and relevant documents.

– Notifications if project data is unavailable or access is restricted.

Performance Requirements

Static: System shall display all projects assigned to the evaluator securely.

Dynamic: 99% of assigned project lists shall load within 2–3 seconds under normal conditions.

Design Constraints

Standards Compliance: Must comply with university data privacy and evaluation policies.

Hardware Limitation: Function operates on existing servers with no additional hardware required.

Attributes

Availability: Function should be available during evaluation periods.

Security: Evaluators can access only their assigned projects; data is protected and access is logged.

Maintainability: Project list display logic can be updated without affecting other modules.

Transferability/Conversion: Can integrate with future evaluation or grading systems.

3.4 Requirement 4: Access Project's Documents

3.4.1 Introduction

This function allows External Evaluators to securely access all documents related to the Final Year Projects assigned to them. It ensures that evaluators can review proposals, progress reports, final reports, presentations, and supporting materials before completing evaluations. The system guarantees that only authorized evaluators can view project documents, maintaining confidentiality and integrity.

Inputs

– Evaluator ID: University-provided credentials to authenticate the evaluator.

– Project ID: Identifier of the assigned project.

– Document Type: Specifies the type of document to be accessed (proposal, report, presentation, etc.).

Processing

Input Validity Checks:

1. System verifies evaluator credentials and confirms project assignment.
2. Checks if the requested document exists and is in a supported format (PDF, DOCX, PPTX).

Sequence of Operations:

1. Evaluator selects the assigned project from their dashboard.
2. System retrieves all associated project documents from the database or file storage.
3. Documents are displayed or downloaded securely for evaluation purposes.

Abnormal Situations:

1. Attempt to access unassigned project documents triggers access denial.
2. Missing or corrupted documents generate an error message.

Parameters Affected:

Document access logs, timestamps, and evaluator activity logs.

Degrade Operation:

System may experience slower document retrieval during peak load or network issues.

Methods Used:

Secure role-based access control (RBAC), encrypted storage, and secure file transfer protocols.

Outputs

– Display or download of project documents to the evaluator.

– Error messages for inaccessible or missing documents.

Performance Requirements

Static: System shall allow evaluators to access all documents of assigned projects securely.

Dynamic: 99% of requested documents shall be accessible within 2–5 seconds under normal conditions.

Design Constraints

Standards Compliance: Must comply with university confidentiality and document management standards.

Hardware Limitation: Function operates on existing servers and storage infrastructure.

Attributes

Availability: Function should be available during evaluation periods.

Security: Documents are accessible only by assigned evaluators; all access is logged and encrypted.

Maintainability: Document access modules can be updated without affecting other system functionalities.

Transferability/Conversion: Can integrate with future document management or grading systems.

3.5 Requirement 5: View Evaluation Deadlines and Schedules

3.5.1 Introduction

This function allows External Evaluators to view all important deadlines and schedules for the evaluation of Final Year Projects assigned to them. It ensures timely evaluation and

proper planning, allowing evaluators to meet university standards and submit assessments within the specified periods.

Inputs

– Evaluator ID: University-provided credentials to authenticate the evaluator.

– Project ID: Identifier for the assigned project(s).

– Schedule Type: Type of schedule or deadline (submission, evaluation, feedback).

Processing

Input Validity Checks:

1. System verifies evaluator credentials and project assignments.
2. Ensures that schedule data exists for the assigned project.

Sequence of Operations:

1. Evaluator logs into the system.
2. Navigates to the "Evaluation Deadlines & Schedules" section.
3. System retrieves all relevant deadlines and schedules from the database.
4. Displays deadlines and schedules in chronological order, with reminders for upcoming tasks.

Abnormal Situations:

1. If the evaluator is not assigned to any projects, the system displays a notification indicating no schedules available.
2. System errors or database unavailability may delay schedule retrieval.

Parameters Affected:

Access logs, timestamps, and notification flags for upcoming deadlines.

Degrade Operation:

During server maintenance or high load, schedule display may be slightly delayed but remains accessible.

Methods Used:

Role-based access control (RBAC), database queries, automated reminders and alerts.

Outputs

– Display of all evaluation deadlines and schedules relevant to the evaluator.

– Notifications or alerts for upcoming submission or evaluation deadlines.

– Error messages if schedules are unavailable or access is unauthorized.

Performance Requirements

Static: System shall allow evaluators to view all project-related deadlines and schedules.

Dynamic: 99% of schedule requests shall be displayed within 2 seconds.

Design Constraints

Standards Compliance: Must follow university academic calendar and evaluation policies.

Hardware Limitation: Operates on existing servers and database systems.

Attributes

Availability: Function should be available throughout the evaluation period.

Security: Only assigned evaluators can view schedules; all access is logged.

Maintainability: Schedule display logic can be updated without affecting other system modules.

Transferability/Conversion: Can be integrated with future automated notification or calendar systems.

3.6 Requirement 6: Submit Evaluation Marks and Remarks

3.6.1 Introduction

This function enables External Evaluators to submit their evaluation scores, comments, and recommendations for assigned Final Year Projects. It ensures fair, accurate, and timely assessment while maintaining academic standards. The system securely records the evaluations and prevents unauthorized changes once submitted.

Inputs

– Evaluator ID: Credentials provided by the university for authentication.

– Project ID: Identifier for the assigned project.

– Evaluation Form: Predefined form including grading rubrics, criteria, and fields for remarks.

– Marks and Remarks: Scores, comments, and suggestions entered by the evaluator.

Processing

Input Validity Checks:

1. Verify evaluator credentials and project assignment.
2. Ensure that all mandatory fields in the evaluation form are completed.
3. Validate marks against allowed ranges defined by university evaluation policies.

Sequence of Operations:

1. Evaluator logs in and accesses the assigned project.
2. Completes the evaluation form with marks and remarks.
3. Submits the evaluation; the system encrypts and stores the data securely.
4. System locks the evaluation form to prevent further edits.

5. Notifications are sent to coordinators and HoD about submission.

Abnormal Situations:

1. Incomplete forms trigger error messages and prevent submission.
2. Unauthorized access attempts are logged and blocked.
3. System or network failure during submission may temporarily prevent data entry; retry options are provided.

Parameters Affected:

Project evaluation records, submission timestamps, audit logs.

Degrade Operation:

Submission may be delayed during high server load but is queued for processing.

Methods Used:

Role-based access control (RBAC), secure database transactions, audit logging.

Outputs

– Confirmation message for successful submission.

– Updated evaluation record accessible to coordinators and HoD.

– Notifications of submission sent to relevant stakeholders.

– Error messages for incomplete forms or unauthorized attempts.

Performance Requirements

Static: System shall allow evaluators to submit marks and remarks for assigned projects.

Dynamic: 99% of evaluation submissions shall be stored and acknowledged within 3–5 seconds.

Design Constraints

Standards Compliance: Must follow university evaluation policies and rubrics.

Hardware Limitation: Operates using existing servers and infrastructure.

Attributes

Availability: Available during evaluation periods only.

Security: Marks and remarks are encrypted; only assigned evaluators can submit.

Maintainability: Evaluation submission logic can be updated without affecting other modules.

Transferability/Conversion: Can integrate with university grading systems in future.

3.7 Requirement 7: View Evaluation Criteria and Instructions

3.7.1 Introduction

This function allows External Evaluators to access the detailed evaluation criteria and instructions provided by the university for assessing Final Year Projects. It ensures that evaluations are consistent, standardized, and aligned with academic policies. Evaluators can refer to rubrics, scoring guidelines, and special instructions for each project.

Inputs

– Evaluator ID: Credentials provided by the university for authentication.

– Project ID: Identifier for the assigned project.

– Evaluation Guidelines Document: Predefined set of rubrics, scoring instructions, and academic policies.

Processing

Input Validity Checks:

1. Verify evaluator credentials and assignment to the project.
2. Ensure that the evaluation criteria document exists for the project.

Sequence of Operations:

1. Evaluator logs into the system.
2. Selects the assigned project.
3. Opens and reviews evaluation criteria, rubrics, and instructions.
4. System tracks access in audit logs.

Abnormal Situations:

1. Unauthorized access triggers an error message and logging.
2. Missing or corrupted evaluation guidelines document generates a notification to administrators.

Parameters Affected:

Access logs, audit trails for evaluator actions.

Degrade Operation:

System may delay document retrieval under high server load; cached copies may be used to maintain access.

Methods Used:

Secure role-based access control, document management system, audit logging.

Outputs

– Display of evaluation criteria and instructions for the assigned project.

– Notifications of missing or updated guidelines sent to evaluators.

– Logged access history for accountability.

Performance Requirements

Static: System shall allow evaluators to view evaluation criteria and instructions for their assigned projects.

Dynamic: 99% of document accesses should occur within 2–3 seconds under normal conditions.

Design Constraints

Standards Compliance: Must follow university evaluation policies and formatting standards.

Hardware Limitation: Operates on existing servers and network infrastructure.

Attributes

Availability: Accessible throughout the evaluation period.

Security: Only assigned evaluators may view criteria; content cannot be modified.

Maintainability: Evaluation instructions can be updated by administrators without affecting the evaluator interface.

Transferability/Conversion: System can integrate with future university evaluation platforms.

3.8 Requirement 8: Submit Marks and Remarks on Projects

3.8.1 Introduction

This function allows External Evaluators to submit final marks and remarks for the projects assigned to them. It ensures that the assessment is recorded securely, aligned with the university's grading policies, and accessible to authorized personnel like coordinators and HoD. The system maintains a record of all submissions for accountability and future reference.

Inputs

– Evaluator ID: Credentials provided by the university.

– Project ID: Identifier for the assigned project.

– Evaluation Marks: Numerical or graded scores according to the evaluation rubric.

– Remarks/Comments: Written feedback, suggestions, or observations for the student's project.

Processing

Input Validity Checks:

1. Verify evaluator's credentials and ensure project assignment.
2. Validate that marks are within the allowed scoring range.
3. Check that remarks are complete and comply with format guidelines.

Sequence of Operations:

1. Evaluator logs into the system.
2. Selects the assigned project.
3. Enters marks and remarks in the submission form.
4. System validates entries and confirms correctness.
5. Submits data to the database and locks the record to prevent modifications.
6. System sends confirmation notifications to coordinators and HoD.
7. Audit logs record submission actions with timestamps.

Abnormal Situations:

1. Unauthorized access attempts trigger access denial and logging.
2. Submission with missing or invalid marks generates an error prompt.
3. Network issues may delay submission; system retries automatically.

Parameters Affected:

Final marks, remarks, submission timestamps, audit logs.

Degrade Operation:

Under heavy load or network issues, submission may be delayed, but cached data ensures no loss.

Methods Used:

Secure role-based access, database transactions, controlled submission workflow, audit logging.

Outputs

– Confirmation message of successful submission.

– Updated project status showing evaluation completion.

– Audit logs capturing evaluator's submission actions.

Performance Requirements

Static: System shall allow external evaluators to submit marks and remarks for assigned projects.

Dynamic: 99% of submissions should be processed and stored within 3–5 seconds under normal conditions.

Design Constraints

Standards Compliance: Must adhere to university evaluation policies and grading standards.

Hardware Limitation: Works with existing servers and infrastructure without additional requirements.

Attributes

Availability: Functional during the evaluation period.

Security: Submissions are encrypted and locked to prevent unauthorized modifications.

Maintainability: Submission workflows can be updated without redesigning the system.

Transferability/Conversion: Can integrate with other university evaluation or reporting systems in the future.