DR. YANGA'S COLLEGES, INC.
182 MACARTHUR HIGHWAY, WAKAS, BOCAUE, BULACAN PH 3018

STUDENT CONSULTATION SYSTEM
DYCI CCS WEB PORTAL

In Partial Fulfillment of the
Requirements in
Advance Information Assurance and Security

Submitted By:
Legaspi, Cristan Irish P.
Mañabat, Trishia Mae L.
Martin, John Andrei M.
Reyes, Jeorge Anthony J.
Yap, John Oswald B.

Submitted To:
Peter Paul Ocampo
AIA Adviser

March 2025

Part 1: Scope and Requirements of Student Consultation System (Feature for CCS Portal)

1. Project Overview

- **Purpose:** The Student Consultation System is a feature within the DYCI CCS Web Portal designed to streamline the scheduling and management of student consultations with professors. It aims to reduce manual coordination, minimize scheduling conflicts, and enhance the overall efficiency of academic consultations. The system will provide a centralized platform for students and professors to manage consultation requests, availability, and records.

- **Target Audience:** The intended users of the system include:
  - Students: Individuals seeking academic guidance or consultations with professors.
  - Professors: Academic staff providing consultations and managing their availability.
  - Administrators: System administrators responsible for maintaining the consultation feature and ensuring its smooth operation.

- **Business Goals**

  The system aims to achieve the following objectives:
  - Improve Efficiency: Automate the consultation scheduling process to save time and reduce manual effort.
  - Enhance Communication: Provide real-time notifications and updates to both students and professors.
  - Increase Accessibility: Offer a user-friendly platform for managing consultations.
  - Maintain Records: Store consultation history and notes for future reference.

2. Functional Requirements

Core Features

1. **Consultation Scheduling**: Students can request a consultation by selecting:
    - Professor
    - Date & Time
    - Consultation Topic/Concern
    - Professors can approve or reject requests.
    - Automatic notifications for confirmed appointments.

2. **Consultation Availability Management**
    - Professors can set their available time slots.
    - Students can only book open slots to prevent scheduling conflicts.

3. **Consultation Records & History**
    - Students and professors can view past consultations.
    - Option to add notes or summaries after each session.

4. **Real-time Notifications**
    - Email or in-system alerts for approved, rescheduled, or canceled consultations.

Optional Features

- Automated Reminders: Sends reminders for upcoming consultations to both students and professors.
- Feedback System: Allows students to rate their consultation experience and provide feedback.

3**. Non-Functional Requirements**

- Performance: The system should handle multiple consultation requests simultaneously without delays.
- Scalability: The system should be scalable to accommodate an increasing number of users and consultations.
- Security: Ensure data privacy and secure access to consultation records.
- Usability: The interface should be intuitive and easy to navigate for both students and professors.

4. System Integrations

- DYCI CCS Portal: Integration with the existing DYCI CCS Web Portal for seamless user access.
- Email Service: Integration with an email service provider for sending notifications and reminders.
- Calendar System: Integration with calendar systems (e.g., Google Calendar) for scheduling and reminders.

5. User Roles and Permissions

- Students: Can request consultations, view past consultations, and receive notifications.
- Professors: Can manage availability, approve/reject requests, view consultation history, and add session notes.
- Administrators: Can manage system settings, user roles, and troubleshoot issues.

6. Technical Requirements

- Frontend: HTML, CSS, JavaScript (Bootstrap for UI)
- Backend: PHP
- Database: MySQL

Part 2: Information Assurance Plan for Server

1. Executive Summary

- Purpose: The Information Assurance (IA) Plan for the Student Consultation System ensures the security, confidentiality, integrity, and availability of data hosted on the Linux VPS. This plan outlines the protocols and controls necessary to safeguard the system and its users.
- Scope: The plan covers the following components:

-Web servers hosting the consultation system.

- Databases storing consultation records and user data.

- File systems and logs.

- Objectives

- Maintain the security and privacy of consultation data.

- Ensure compliance with relevant regulations (e.g., GDPR, FERPA).

- Guarantee the availability and reliability of the system.

2. Security Policies

- Security Governance

- Define acceptable use policies for the system.

- Establish incident response procedures for security breaches.

- Roles and Responsibilities

- System Administrators: Responsible for server maintenance, updates, and access control.

- Security Personnel: Monitor system activity and respond to security incidents.

- Users: Adhere to security policies and report suspicious activity.

- Regulatory Compliance

- Ensure compliance with data protection regulations such as GDPR (General Data Protection Regulation) and FERPA (Family Educational Rights and Privacy Act).

3. System Hardening and Configuration

- Operating System Hardening

- Reduce the number of installed packages to minimize vulnerabilities.
- Disable unnecessary services and ports.
- Assign appropriate file system permissions.
- Regularly update the system with security patches.

- Security Tools

- Implement tools such as SELinux, AppArmor, iptables, fail2ban, and auditd to enhance security.

- SSH Security

- Disable root login via SSH.
- Mandate the use of SSH keys instead of passwords.
- Use a non-standard SSH port.
- Restrict SSH access through firewall rules and IP whitelisting.

4. Access Control

- Authentication

- Require strong, complex passwords for all accounts.
- Implement multi-factor authentication (MFA) for critical access (e.g., SSH).

- User Privileges and Role-Based Access Control (RBAC)

- Enforce the principle of least privilege (PoLP).
- Use sudo for elevated permissions instead of logging in as root.

- User Account Management

- Regularly review and disable inactive or outdated user accounts.

- Audit Trails

- Activate system logging (via syslog or rsyslog).
- Maintain comprehensive logs of system access and modifications, including authentication attempts and administrative actions.