| Network Security and Compliance |
| --- |

Date: June 1st 2024

Revision: 1.0

**Table of Contents**

1. **Introduction**
   * Objective
   * Scope
2. **Security Measures**
   * Authentication and Authorization
     + Multi-Factor Authentication (MFA)
     + Role-Based Access Control (RBAC)
   * Data Encryption
     + Encryption in Transit
     + Encryption at Rest
   * Secure Development Practices
     + Code Review and Testing
     + Vulnerability Management
   * Network Security
     + Firewalls
     + Intrusion Detection and Prevention Systems (IDPS)
   * Incident Response
     + Incident Detection
     + Response and Recovery Procedures
3. **Compliance Strategies**
   * Regulatory Frameworks
     + FERPA (Family Educational Rights and Privacy Act)
     + GDPR (General Data Protection Regulation)
     + CCPA (California Consumer Privacy Act)
   * Data Privacy
     + Student Data Protection
     + Data Retention Policies
   * Accessibility Compliance
     + ADA (Americans with Disabilities Act)
     + WCAG (Web Content Accessibility Guidelines)
4. **Application-Specific Security Measures**
   * Course Management System
     + Secure Registration and Drop Processes
     + Scheduling and Timetable Management Security
   * Grading System
     + Secure Submission and Review Mechanisms
     + Plagiarism Detection and Reporting Security
   * Notification System
     + Secure Messaging and Notification Channels
     + Data Protection in Notifications
   * Analytics System
     + Secure Data Aggregation and Analysis
     + Capacity Planning Security Measures
5. **Implementation Plan**
   * Security Policies
   * Training and Awareness Programs
   * Continuous Monitoring and Improvement
6. **Conclusion**
   * Summary of Security and Compliance Strategies
   * Future Considerations

| **SOW Reference** | TEAM # 1 /2024-06/001 | **Professor** | **Yang Sun**  [**Yangsun.com@gmail.com**](mailto:Yangsun.com@gmail.com) |
| --- | --- | --- | --- |
| **Project Title** | **TEAM # 1**  **Network Security and Compliance** |
| **Team Members Email ID** | **Yilun Jin**  **Maheswar Barrenkala**  **Akshat Jangam**  **Atilla Karaali**  **Shital Hinge**  **Jean Qiong Zhang**  **Caihui Yang**  **Dhruv Basnotra**  **Xu Liu** | **Team Members Email ID** | [**karen.jin.job@gmail.com**](mailto:karen.jin.job@gmail.com)  [**maheswar.barrenkala@gmail.com**](mailto:maheswar.barrenkala@gmail.com)  [**akshat.ja@gmail.com**](mailto:akshat.ja@gmail.com)  [**atilla.karaali@gmail.com**](mailto:atilla.karaali@gmail.com)  [**Shitalkarleg@gmail.com**](mailto:Shitalkarleg@gmail.com)  [**jzhang95014@gmail.com**](mailto:jzhang95014@gmail.com)  [**ashleyyang924@gmail.com**](mailto:ashleyyang924@gmail.com)  [**dhruvbasnotra@gmail.com**](mailto:dhruvbasnotra@gmail.com)  **liuxubupt16@gmail.com** |

| **Security and Compliance Report for University Web Application****Index****1. Introduction****Objective** This report outlines the security measures and compliance strategies for the university web application designed for students, professors, and IT administrators. The objective is to ensure the implementation of security best practices and adherence to industry regulations within the education technology sector. **Scope** The report covers security and compliance strategies for core functional requirements: Course Management System, Grading System, Notification System, and Analytics System. **2. Security Measures****Authentication and Authorization**Multi-Factor Authentication (MFA) Implement MFA to ensure that only authorized users can access sensitive parts of the application. This adds an extra layer of security by requiring users to provide two or more verification factors. Role-Based Access Control (RBAC) Use RBAC to assign permissions based on the user's role within the university, ensuring that students, professors, and IT admins have appropriate access levels. **Data Encryption**Encryption in Transit Encrypt data transmitted between users and the server using TLS (Transport Layer Security) to prevent interception by unauthorized parties. Encryption at Rest Encrypt data stored in databases to protect it from unauthorized access, using strong encryption algorithms such as AES-256. **Secure Development Practices**Code Review and Testing Conduct regular code reviews and security testing, including static and dynamic analysis, to identify and mitigate vulnerabilities in the application. Vulnerability Management Implement a vulnerability management program to regularly scan for and address security weaknesses, ensuring timely updates and patches. **Network Security**Firewalls Deploy firewalls to protect the application from unauthorized access and monitor incoming and outgoing traffic based on predetermined security rules. Intrusion Detection and Prevention Systems (IDPS) Use IDPS to detect and prevent malicious activities by monitoring network traffic and application behavior for signs of security breaches. **Incident Response**Incident Detection Set up systems to detect security incidents promptly through continuous monitoring and automated alerts. Response and Recovery Procedures Develop and implement procedures for responding to and recovering from security incidents, minimizing impact and restoring normal operations quickly. **3. Compliance Strategies****Regulatory Frameworks**FERPA (Family Educational Rights and Privacy Act) Ensure compliance with FERPA to protect the privacy of student education records, including secure handling, access control, and data sharing protocols. GDPR (General Data Protection Regulation) Adhere to GDPR requirements for handling personal data of EU students, including data subject rights, lawful processing, and data protection impact assessments. CCPA (California Consumer Privacy Act) Comply with CCPA regulations to protect the privacy of California residents' personal information, including transparency, access, and deletion rights. **Data Privacy**Student Data Protection Implement robust measures to protect student data, ensuring confidentiality, integrity, and availability. Data Retention Policies Establish clear data retention policies to determine how long different types of data should be retained and securely disposed of when no longer needed. **Accessibility Compliance**ADA (Americans with Disabilities Act) Ensure the application is accessible to all users, including those with disabilities, by complying with ADA requirements. WCAG (Web Content Accessibility Guidelines) Adopt WCAG standards to make the application accessible to a wider range of people with disabilities, including visual, auditory, and cognitive impairments. **4. Application-Specific Security Measures****Course Management System**Secure Registration and Drop Processes Implement secure mechanisms for course registration and dropping to prevent unauthorized changes and data manipulation. Scheduling and Timetable Management Security Ensure the scheduling and timetable management system is secure, preventing unauthorized access and modification of class schedules. **Grading System**Secure Submission and Review Mechanisms Secure the submission and review processes to ensure the integrity and confidentiality of student work and feedback. Plagiarism Detection and Reporting Security Protect the plagiarism detection system to ensure accurate reporting and prevent unauthorized access to student submissions. **Notification System**Secure Messaging and Notification Channels Securely transmit notifications and messages to prevent interception and unauthorized access. Data Protection in Notifications Ensure that sensitive information included in notifications is protected and only accessible to intended recipients. **Analytics System**Secure Data Aggregation and Analysis Protect the data aggregation and analysis processes to maintain the integrity and confidentiality of analytics data. Capacity Planning Security Measures Implement security measures for capacity planning to ensure that student and class data is protected during analysis and decision-making processes. **5. Implementation Plan****Security Policies** Develop and enforce security policies that define the security requirements and procedures for the application. **Training and Awareness Programs** Conduct regular training and awareness programs for students, professors, and IT admins to promote security best practices and compliance. **Continuous Monitoring and Improvement** Implement continuous monitoring and improvement processes to ensure the application remains secure and compliant with evolving regulations and threats. **6. Conclusion****Summary of Security and Compliance Strategies** This report outlines comprehensive security measures and compliance strategies to protect the university web application, ensuring the confidentiality, integrity, and availability of data while adhering to industry regulations. **Future Considerations** Regularly review and update security and compliance measures to address emerging threats and changes in regulatory requirements, maintaining the highest standards of protection for the university community.  This report provides a detailed outline for implementing security measures and compliance strategies tailored to the core functional requirements of the university web application. By following this plan, the application can ensure robust security and compliance, protecting the interests of all stakeholders involved.  END |
| --- |