

Security Requirements Generated (GEN1+GEN2)

1. Implement role-based access control to ensure students, professors, and course coordinators can only access relevant data and functionalities. – Access Management
2. Ensure that unauthorized users cannot modify class schedules or exam bookings. – Web Application Security
3. Validate that users can only view their own course schedules and calendar entries. – Input Validation
4. Sanitize all user inputs to prevent SQL injection attacks when searching for class schedules or booking exam sessions. – Input Validation
5. Use parameterized queries to prevent injection vulnerabilities in database interactions. – Secure Coding
6. Validate and escape all user-generated content before displaying it on the platform. – Web Application Security
7. Ensure that all sensitive data, such as passwords and user messages, are encrypted both in transit and at rest. – Data Protection
8. Implement secure session management to prevent session hijacking. – Web Application Security
9. Use HTTPS protocol for all communications to protect data integrity and confidentiality. – Secure Design
10. Implement multi-factor authentication for professors and course coordinators to enhance account security. – Authentication
11. Ensure that passwords are hashed using a strong cryptographic algorithm before storage. – Data Protection
12. Provide secure password recovery mechanisms to prevent unauthorized access. – Privacy Security
13. Conduct regular security audits to identify and mitigate vulnerabilities in the platform. – Security Testing
14. Monitor and log all access attempts to detect and respond to unauthorized access. – Access Management
15. Ensure that the platform is available and responsive during peak usage times. – Availability
16. Implement multi-factor authentication for all user accounts. – Authentication
17. Ensure password complexity requirements are enforced during account creation. – Authentication
18. Implement session timeout and automatic logout after inactivity. – Authentication
19. Ensure the platform can handle a minimum of 10,000 concurrent users without degradation in performance. – Availability
20. Implement load balancing to distribute traffic evenly across servers. – Availability

21. Set up automated failover mechanisms to maintain uptime during server failures. – Availability
22. Encrypt all sensitive data at rest using AES-256 encryption. – Privacy Security
23. Ensure all data transmitted between the client and server is encrypted using TLS 1.2 or higher. – Privacy Security
24. Implement role-based access control to restrict access to sensitive information. – Privacy Security
25. Conduct regular code reviews to identify and fix security vulnerabilities. – Secure Coding
26. Use parameterized queries to prevent SQL injection attacks. – Secure Coding
27. Sanitize all user inputs to prevent cross-site scripting (XSS) attacks. – Secure Coding
28. Design the system with a zero-trust architecture to minimize attack surfaces. – Secure Design
29. Implement secure default configurations for all system components. – Secure Design
30. Ensure all third-party libraries are vetted for security vulnerabilities before integration. – Secure Design
31. Perform penetration testing biannually to identify and mitigate security risks. – Security Testing
32. Conduct automated security scans on all code commits to detect vulnerabilities early. – Security Testing
33. Implement continuous monitoring to detect and respond to security incidents in real-time. – Security Testing

Total: GEN1=15, GEN2=18, Total=33

Counting per category (total = gen1 + gen2):

- Access Management: total=2 (gen1=2, gen2=0)
- Authentication: total=4 (gen1=1, gen2=3)
- Availability: total=4 (gen1=1, gen2=3)
- Data Protection: total=2 (gen1=2, gen2=0)
- Input Validation: total=2 (gen1=2, gen2=0)
- Privacy Security: total=4 (gen1=1, gen2=3)
- Secure Coding: total=4 (gen1=1, gen2=3)
- Secure Design: total=4 (gen1=1, gen2=3)
- Security Testing: total=4 (gen1=1, gen2=3)
- Web Application Security: total=3 (gen1=3, gen2=0)