Development Security Practices and Standards

Security Practices and Standards for the Development Process

Introduction

This document outlines the security practices and standards to guide the development of our new solution, which must:

- Display videos, images, and text.
- Edit display duration for each post.
- Easily add content from mobile and PC.
- Archive expired content for potential future use.
- Allow an admin (or possibly all users) to edit others' content.

The solution is designed to share important information on an office screen.

Security Principles

- **Confidentiality**
  - Protect all sensitive information from unauthorized access.
- **Integrity**
  - Ensure systems and data are protected from unauthorized changes or deletion.
- **Availability**
  - Make sure the system is accessible to authorized users when needed.

Security Practices

- **Secure Development Lifecycle (SDLC)**
  - Integrate security into all phases of development:
- **Requirements Phase**
  - Identify and document security requirements.
- **Design Phase**
  - Perform threat modeling and security design reviews.
- **Implementation Phase**
  - Follow secure coding standards and practices.
  - Implement strong authentication and authorization.
- **Testing**
  - Conduct static and dynamic security testing.
  - Test access controls and data integrity.
- **Deployment**
  - Secure the deployment environment and test for security vulnerabilities.
  - Implement secure update mechanisms.
- **Maintenance**
  - Continuously monitor security and apply updates regularly.
  - Perform regular security audits.

2. Security Architecture

- Implement layered security (Defense-in-Depth).
- Use the principle of least privilege for access control.
- Encrypt data in transit (TLS/SSL) and at rest.

3. Coding Standards

- Follow established secure coding standards like OWASP.
- Regularly conduct security-focused code reviews.
- Use static code analysis tools to find vulnerabilities.

4. Vulnerability Management

- Regularly perform security scans and penetration testing.
- Implement a process to prioritize and fix vulnerabilities.
- Keep the system updated with security patches.

5. Security Awareness

- Provide regular security training for the development team.
- Keep developers informed about current security threats and best practices.

Standards

1. Authentication and Authorization

- Use strong authentication mechanisms like multi-factor authentication (MFA).
- Implement robust authorization controls based on roles and needs.

2. Logging and Monitoring

- Implement comprehensive logging of security events and activities.
- Continuously monitor systems for suspicious activity.

3. Security Assessments

- Regularly conduct security audits and assessments.
- Perform risk analyses to identify and mitigate potential security risks.

4. Incident Response

- Develop and maintain an incident response plan.
- Regularly test and improve the incident response process.

Compliance

- Ensure the development process and solution comply with relevant laws and regulations.
- Follow industry standards and guidelines, such as ISO 27001 and GDPR.

Conclusion

By following to these security practices and standards, we ensure our new solution is developed with high security standards, protecting our organization and users from potential threats. This fosters trust and ensures a reliable platform for sharing information in the office.