Secure Application Development Lifecycle

A structured framework designed to integrate security practices within every phase of the application development process. This playbook ensures that security considerations are embedded from the initial planning to the deployment and maintenance stages of software development.

Step 1: **Planning**

Identify security requirements and integrate them into the application design. Perform risk assessments to determine the security posture needed for the application.

Step 2: **Design**

Incorporate security into the application architecture. Design the application with secure coding practices in mind, and ensure that the design complies with regulatory and policy requirements.

Step 3: **Development**

Follow secure coding guidelines to write the application code. Continuously check for and fix security vulnerabilities within the codebase.

Step 4: **Testing**

Execute security testing protocols to identify any security issues. This includes performing code reviews, static and dynamic analysis, and penetration testing.

Step 5: **Deployment**

Prior to deployment, ensure all security checks are completed and the application is compliant with security policies. Roll out the application in a controlled environment.

Step 6: **Maintenance**

Continuously monitor the application for security threats. Regularly update the software, patch vulnerabilities, and revise security measures as necessary.

Step 7: **Incident Response**

Have an incident response plan in place to deal with potential security breaches. Regularly test and update this plan to ensure its effectiveness in the event of an actual incident.

General Notes

Compliance

Ensure compliance with all relevant legal, regulatory, and policy frameworks related to security throughout the lifecycle.

Training

Provide ongoing security training and awareness for the development team to reinforce the importance of security measures and keep up to date with the latest threats and technologies.

Documentation

Maintain thorough documentation of all security measures, incidents, and operating procedures to support transparency and facilitate audits.