## **ISO 27001 Software Development Life Cycle (SDLC) Policy Template**

### **1. Introduction**

This document outlines the Software Development Life Cycle (SDLC) Policy for [Organization Name], ensuring compliance with ISO/IEC 27001:2022 requirements. The policy provides a framework for secure software development to mitigate risks and protect organizational assets.

### **2. Purpose**

The purpose of this policy is to:

1. Define secure practices for software development, testing, and deployment.
2. Ensure compliance with ISO 27001 standards and other relevant regulations.
3. Minimize vulnerabilities and risks throughout the software development lifecycle.
4. Enhance software quality and security.

### **3. Scope**

This policy applies to all software development activities within [Organization Name], including:

* Internal and third-party software development.
* Applications and systems used for business operations.
* Development, testing, and production environments.

### **4. Policy Statement**

[Organization Name] is committed to implementing secure SDLC practices to protect its software and systems. This includes:

1. Adhering to secure coding standards.
2. Conducting regular security testing.
3. Ensuring proper documentation and review at all SDLC phases.

### **5. SDLC Phases and Security Requirements**

#### **5.1 Requirements Gathering**

1. Identify and document functional, performance, and security requirements.
2. Conduct a preliminary risk assessment for potential threats.

#### **5.2 Design**

1. Develop secure architecture and design based on identified requirements.
2. Perform threat modeling to identify and address security gaps.

#### **5.3 Development**

1. Follow secure coding standards, such as OWASP.
2. Use version control systems with access controls and activity logs.
3. Perform static application security testing (SAST) to identify vulnerabilities in code.

#### **5.4 Testing**

1. Conduct dynamic application security testing (DAST) and penetration testing.
2. Ensure all identified vulnerabilities are addressed before deployment.
3. Document testing results and corrective actions.

#### **5.5 Deployment**

1. Deploy software using automated and secure pipelines.
2. Implement rollback mechanisms for failed deployments.
3. Validate that all configurations meet security standards.

#### **5.6 Maintenance**

1. Apply patches and updates regularly to address vulnerabilities.
2. Monitor software performance and security continuously.
3. Conduct periodic security reviews and audits.

### **6. Roles and Responsibilities**

1. **Development Team:** Follow secure coding practices and address identified vulnerabilities.
2. **QA Team:** Perform rigorous testing to ensure software meets security and performance standards.
3. **Information Security Officer (ISO):** Oversee security controls throughout the SDLC.
4. **Project Managers:** Ensure compliance with this policy and manage SDLC timelines.
5. **System Administrators:** Maintain secure environments for development, testing, and deployment.

### **7. Compliance and Monitoring**

1. Conduct regular audits to ensure adherence to this policy.
2. Monitor development activities for potential security violations.
3. Address non-compliance through corrective actions or disciplinary measures.

### **8. Related Documentation**

1. Information Security Policy
2. Risk Management Policy
3. Incident Management Policy

### **9. Review and Revision**

This policy will be reviewed annually or upon significant changes to the SDLC process or tools. Updates will be approved by the Information Security Officer.

### **Appendix A: Secure Coding Checklist**

| **Area** | **Checklist Item** | **Compliance Status** |
| --- | --- | --- |
| Input Validation | Validate all user inputs |  |
| Authentication | Use multi-factor authentication |  |

### **Appendix B: SDLC Phase Checklist**

| Phase | Key Activities | Responsible Team | Completion Date |
| --- | --- | --- | --- |
| Requirements | Document all functional and security needs | Development Team |  |

### **Appendix C: Policy Acknowledgment Form**

I acknowledge that I have read and understood the SDLC Policy and agree to comply with its requirements.

**Name:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
**Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
**Date:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_