## **ISO 27001 CI/CD Policy Template**

### **1. Introduction**

This document outlines the Continuous Integration and Continuous Deployment (CI/CD) Policy for [Organization Name], ensuring compliance with ISO/IEC 27001:2022 requirements. The policy establishes a secure framework for automating software integration, testing, and deployment to protect the organization’s information assets. For example, a secure CI/CD process can mitigate risks such as unauthorized code changes or deployment failures.

### **2. Purpose**

The purpose of this policy is to:

1. Ensure secure development and deployment practices in alignment with ISO 27001 standards.
2. Minimize risks associated with software vulnerabilities, deployment failures, and unauthorized access.
3. Define roles and responsibilities for CI/CD processes.
4. Enhance operational efficiency while maintaining robust security controls.

### **3. Scope**

This policy applies to all software development, testing, and deployment activities conducted within [Organization Name]. It encompasses:

* CI/CD pipelines and associated tools, such as Jenkins or GitHub Actions.
* Source code repositories.
* Build, testing, staging, and production environments.

### **4. Policy Statement**

[Organization Name] commits to implementing secure and compliant CI/CD practices to maintain the integrity, confidentiality, and availability of its software systems. All CI/CD processes must follow this policy, including:

1. Secure access to code repositories and pipelines.
2. Regular testing and validation of software before deployment.
3. Monitoring and logging of all CI/CD activities, aligned with industry standards such as OWASP.

### **5. Roles and Responsibilities**

1. **Development Team:** Write secure code, submit changes, and review pipeline execution.
2. **DevOps Team:** Design, implement, and maintain CI/CD pipelines, ensuring compliance with security standards and coordinating with the ISO.
3. **Information Security Officer (ISO):** Review and approve security controls within CI/CD processes.
4. **System Administrators:** Secure deployment environments and monitor system performance.
5. **Development Team:** Write secure code, submit changes, and review pipeline execution.
6. **DevOps Team:** Design, implement, and maintain CI/CD pipelines, ensuring compliance with security standards.
7. **Information Security Officer (ISO):** Review and approve security controls within CI/CD processes.
8. **System Administrators:** Secure deployment environments and monitor system performance.

### **6. Compliance and Monitoring**

1. Conduct regular audits to ensure CI/CD practices comply with this policy and ISO 27001 requirements.
2. Monitor pipeline activities for unauthorized actions or anomalies.
3. Document and review incidents related to CI/CD pipelines.

### **7. Related Documentation**

1. Change Management Policy
2. Software Development Life Cycle (SDLC) Policy
3. Information Security Policy

### **8. Review and Revision**

This policy will be reviewed annually or upon significant changes to CI/CD processes or tools. Revisions will be approved by the Information Security Officer.

### **Appendix A: Pipeline Security Checklist**

| **Area** | **Checklist Item** | **Compliance Status** |  |
| --- | --- | --- | --- |
| Code Repository Access | Ensure role-based access control is implemented. | Build Environment | Secure build environment against unauthorized access. |

Example: For instance, a completed entry might look like:

### **Appendix B: Incident Report Template**

| Incident ID | Date/Time | Description of Incident | Actions Taken | Resolution Status |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |

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

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

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