1. Introduction

This policy defines the organization's approach to managing third-party developers (Suppliers) contributing to software development projects. It ensures that third-party developers adhere to the organization's security, legal, and performance standards throughout the software development lifecycle.

This policy applies to all third-party vendors, contractors, and external development teams involved in software development, integration, maintenance, or testing for the organization. It covers all software systems' development, deployment, and management activities.

Roles and Responsibilities

- **Third-Party Developers:** Responsible for complying with the organization's policies, security standards, and contractual obligations.
- **Vendor Management Team:** Oversees third-party developers' selection, onboarding, and monitoring.
- **Security Team:** Ensures third-party developers follow security guidelines and evaluate their adherence to security standards.
- **Legal Team:** Reviews and approves contracts, including non-disclosure agreements (NDAs), data protection agreements, and intellectual property clauses.
- **Project Managers:** Coordinate third-party activities, ensure deliverables meet standards, and liaise between third-party developers and internal teams.

2. Policy

2.1 Vendor Selection and Evaluation

- **Due Diligence:** Before engaging third-party developers, the organization will conduct due diligence to assess the vendor's capabilities, security practices, reputation, and compliance with industry standards (e.g., ISO 27001, SOC 2, or similar).
- **Risk Assessment:** A risk assessment must evaluate the potential security, operational, and financial risks of engaging third-party developers. This assessment should include a review of past security incidents, data protection practices, and regulatory compliance.
- **Background Checks:** Ensure that third-party developers and their personnel have passed background checks as necessary, especially for sensitive or high-security projects.

2.2 Contractual Obligations

- **Service Level Agreements (SLAs):** Establish SLAs that define performance expectations, timelines, security responsibilities, and penalties for non-compliance. These SLAs must be included in contracts with third-party developers.
- **Non-Disclosure Agreements (NDAs):** All third-party developers must sign NDAs to protect the organization's confidential information and intellectual property.
- **Data Protection Agreements:** Include data protection clauses to ensure compliance with relevant data privacy laws (e.g., GDPR, CCPA). Third-party developers must agree to secure the organization's data in line with applicable privacy regulations.

- **Intellectual Property Rights:** Ensure that contracts clearly outline the ownership of intellectual property (IP) developed by third-party developers. Unless otherwise agreed, the organization should retain full ownership of any code, designs, or products developed.
- **Termination and Exit Clauses:** Contracts must include termination clauses that define the process for discontinuing the relationship and transferring responsibilities, ensuring the smooth transition of intellectual property and data.

2.3 Onboarding and Training

- **Security Training:** Third-party developers must receive security training on the organization's policies, including secure coding practices, data privacy, and incident reporting procedures. Training should also cover any industry-specific regulations, such as HIPAA or PCI-DSS.
- **Access Management:** Limit third-party access to systems, data, and networks based on the principle of least privilege. Access should only be granted to the resources necessary for the third party to perform their job, and this should be revoked once it is no longer needed.
- **Environment Isolation:** Where feasible, third-party developers should work in isolated environments separate from production systems to reduce the risk of data exposure or accidental impact on live operations.

2.4 Security Requirements

- **Secure Development Practices:** Third-party developers must adhere to the organization's secure software development lifecycle (SSDLC), which includes secure coding practices, vulnerability assessments, and testing.
- **Third-Party Software and Components:** The security team must review and approve any third-party libraries, frameworks, or software third-party developers use and regularly scan them for vulnerabilities.
- **Code Reviews and Audits:** All code developed by third-party developers must undergo internal code reviews and security audits. The organization reserves the right to review and inspect third-party code for security vulnerabilities, performance issues, or non-compliance with standards.
- **Encryption:** Sensitive data must be encrypted in transit and at rest when accessed or handled by third-party developers. Secure protocols (e.g., HTTPS, TLS) must be used to protect data transfers.
- **Incident Reporting:** Third-party developers must report security incidents immediately to the organization's security team. This includes data breaches, unauthorized access, and any suspected vulnerabilities.

2.5 Monitoring and Compliance

- **Continuous Monitoring:** The organization will continuously monitor third-party developer activities, including access logs, system interactions, and adherence to security protocols. Any anomalies or potential security violations will be investigated.
- **Performance Reviews:** Conduct periodic reviews of third-party performance, including adherence to SLAs, project deliverables, and compliance with security policies.
- **Compliance Audits:** Third-party developers must agree to undergo security and compliance audits by the organization or an external auditor if required. This ensures compliance with regulatory requirements, contractual obligations, and internal security standards.

- **Security Testing:** The organization may require third-party developers to participate in security testing such as penetration tests, code scans, and vulnerability assessments to ensure their work meets the organization's security standards.

2.6 Data Protection and Privacy

- **Data Access and Usage:** Third-party developers must ensure access to the organization's sensitive data is authorized, limited, and used strictly for agreed-upon purposes. Data access must comply with all applicable privacy laws and organizational policies.
- **Data Retention and Disposal:** Upon completion of the project or termination of the contract, third-party developers must return or securely destroy all sensitive data, including code, documentation, and test data, as per the organization's data retention policies.
- **Data Breach Notification:** In the event of a data breach or loss of sensitive information, third-party developers must notify the organization immediately and cooperate with the organization's incident response and mitigation efforts.

2.7 Termination and Offboarding

- **Revocation of Access:** Upon contract termination or completion of services, the organization must revoke all access to systems, data, and networks previously granted to the third-party developers. This includes removing access credentials, tokens, and keys.
- **Transfer of Code and Assets:** As part of the termination process, third-party developers must hand over all project-related code, documentation, intellectual property, and other assets.
- **Post-Termination Audits:** The organization may audit the third party's activities post-termination to ensure that all data and assets have been appropriately returned or destroyed and that no security risks remain.

2.8 Dispute Resolution and Legal Actions

- **Dispute Resolution:** In case of disputes regarding performance, security issues, or contract compliance, the organization will follow the dispute resolution process defined in the contract, which may include mediation, arbitration, or legal action.
- **Legal Actions:** The organization reserves the right to take legal action if the third-party developer fails to meet contractual obligations or is involved in any activities that harm the organization's reputation, security, or intellectual property.

4. Enforcement

Failure to comply with this policy or associated contractual agreements will result in contract termination, financial penalties, and legal action. Any security breach by third-party developers may also lead to civil or criminal liability.

5. Review and Updates

This policy will be reviewed annually or when significant changes in the regulatory environment, business operations, or security threats occur. Any updates will be communicated to all third-party developers and relevant stakeholders.

6. Reference

Documents
Secure Development Policy