Wipro’s

Secure Software Development and Maintenance

Lifecycle Policy

**Document Control**

|  |  |
| --- | --- |
| Function | Group Chief Information Security Office (GCISO) |
| Sub-function | - |
| Policy Owner | Lakshminarayanan RS, Group Head - Information Security Policy & Framework |
| Policy Effective Date | July 1, 2002 |

**Purpose**

This policy governs the implementation of information security requirements throughout the information systems development and maintenance life cycle.

**Audience**

Organization’s employees, retainers, contractors, and service providers.

**Scope**

This policy applies to the information systems developed, owned, or managed by the Organization.

**Policy Details**

**SDM.1 The information systems owner shall adhere to the following in the requirement identification phase:**

**SDM.1.1** Information security requirements shall be identified as per the applicable laws, regulations, and business requirements.

**SDM.1.2** Information security risk assessments shall be performed throughout the development and maintenance lifecycle of the information systems.

**SDM.1.3** The data processed in the information systems shall be classified as per the Information Classification, Labelling and Handling Policy.

**SDM.2 Design and Development Team shall adhere to the following:**

**SDM.2.1** Threat modeling shall be performed to identify threats and vulnerabilities and develop security controls to mitigate such threats.

**SDM.2.2** Secure engineering principles shall be considered as per the Secure Coding Standard.

**SDM.2.3** Developers shall have adequate knowledge of the secure coding practices and shall comply with the Secure Coding Standard.

**SDM.2.4** DevSecOps practices shall be followed in the information systems development.

**SDM.2.5** Secure development of the Application Programming Interface (API) shall be performed as per the Application Programming Interface (API) Security Standard.

**SDM.2.6** Tools used in the information systems development shall be securely configured and maintained.

**SDM.2.7** Secure code reviews shall be performed as per the Secure Coding Standard.

**SDM.2.8** The access to source code repositories, development tools, and software libraries shall be secured.

**SDM.2.9** Static Application Security Testing (SAST), Dynamic Application Security Testing (DAST), or Software Composition Analysis (SCA) shall be performed during and after the development as per the business requirements.

**SDM.3 The Testing Team shall adhere to the following:**

**SDM.3.1** Updates and upgrades to the information systems shall be tested and verified during the information system’s development.

**SDM.3.2** Test data shall be appropriately selected, protected, and managed in the testing environment.

**SDM.3.3** Validation checks shall be performed on input and output data.

**SDM.3.4** A security architecture review shall be performed for the information systems prior to production deployment.

**SDM.4 The information systems owner shall ensure the maintenance of the following:**

**SDM.4.1** Aninventory of the information systems shall be maintained in the repository.

**SDM.4.2** Periodic vulnerability scans and risk assessments shall be performed, including privacy by design and periodic privacy assessments.

**SDM.4.3** Identified vulnerabilities shall be remediated throughout the information systems development and maintenance lifecycle.

**SDM.4.4** Changes to the information systems shall be implemented as per the Change Management Policy.

**SDM.4.5** Production, development, and testing environments shall be isolated with relevant access controls.

**SDM.4.6** The information systems shall have a Business Continuity Plan (BCP) and a Disaster Recovery (DR) plan as per the business requirements.

**SDM.5** Contractors and service providers shall comply with the Secure Coding Standard for outsourced development of the information systems.

**SDM.6** Thedevelopment, integration, and testing tools shall be patched as per the Security Patch Management Policy.

**SDM.7** Backup of the source code repository, development, and testing environments shall be performed as per the business requirements.

**SDM.8** Security event logging and monitoring of the information systems, source code repository, development, and testing environments shall be enabled.

**SDM.9** Decommissioned information systems shall be disposed of as per the Asset Management Procedure.

**Definitions**

|  |  |
| --- | --- |
| Definition | Description |
| Business Continuity Plan (BCP) | The documentation of a predetermined set of instructions or procedures that describe how an Organization’s mission or business processes will be sustained during and after a significant disruption. |
| Disaster Recovery (DR) | A plan for recovering information systems at an alternate facility in response to a major failure or destruction of facilities. |
| Dynamic Application Security Testing (DAST) | A method of security testing in which testers examine the information systems while running the tests without knowledge of internal interactions or designs at the system level and without access or visibility to the source code. |
| DevSecOps | Development practice that integrates security testing at each stage of the software development lifecycle to deliver secure information systems. |
| Information Systems | Set of applications, services, information technology assets, or other information-handling components. |
| Organization | Wipro Limited including subsidiaries, affiliates and acquired entities but excluding acquired entities governed by an independent set of security policies. |
| Penetration Testing | A testing methodology in which assessors, typically working under specific constraints, attempt to circumvent the security features of the information systems. |
| Static Application Security Testing (SAST) | A method of security testing designed to analyze the information systems source code, byte code, and binaries for coding and design conditions that are indicative of security vulnerabilities. |
| Software Composition Analysis (SCA) | An automated process that identifies the open-source software in a codebase. SCA analysis is performed to evaluate security, license compliance, and code quality. |
| Secure Engineering Principles | Principles that provide guidance on security aspects. e.g., user authentication techniques, secure session control, data validation, and sanitization. |
| Vulnerability | A weakness in information systems, system security procedures, or internal controls that could be exploited or triggered by a threat source. |

**Acronyms**

|  |  |
| --- | --- |
| Acronym | Description |
| API | Application Programming Interface |
| BCP | Business Continuity Plan |
| DAST | Dynamic Application Security Testing |
| DR | Disaster Recovery |
| GCISO | Group Chief Information Security Office |
| SCA | Software Composition Analysis |
| SAST | Static Application Security Testing |

**References**

* Information Security Policy
* Data Protection and Privacy Policy (Personally Identifiable Information)
* Backup and Restoration Policy
* Change Management Policy
* [Information Classification, Labelling and Handling Policy](https://wiprocio.service-now.com/irm?id=suraksha_kb_article_view&sys_id=9971b7fadb326d181cb2022cd39619dd)
* Security Patch Management Policy
* Application Security Standard
* Application Programming Interface (API) Security Standard
* Logging and Monitoring Standard
* Secure Coding Standard
* Secure Software Development and Maintenance Lifecycle Standard
* Asset Management Procedure
* Secure Software Development and Maintenance Lifecycle Procedure

**Revision History**

| **Version** | **Revision Date** | **Reason for Change** | **Drafted/ Reviewed By** | Approved By | **Date Approved** |
| --- | --- | --- | --- | --- | --- |
| 1.0 | 12th July 2023 | “Application Security Policy” merged with “System Acquisition, Development and Maintenance Policy” and renamed as “Secure Software Development and Maintenance Lifecycle Policy”.  Reviewed and updated the policy as per the ISO 27001:2022 and best practices of NIST 800-53 Rev5. | Jyotisman Chakrabarty/ Maruthi Kumar | Lakshminarayanan RS | 18th January 2024 |