Wipro’s

Configuration Management 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 | March 1, 2022 |

**Purpose**

This policy governs the security configuration process of information systems and protects from unauthorized changes.

**Audience**

Organization’s employees, retainers, contractors, and service providers engaged in configuration management.

**Scope**

This policy is applicable to the information systems owned or managed by the Organization.

**Policy Details**

**CM.1** Security Baseline Configuration requirements for the information systems shall be defined and documented as per industry standards and business requirements.

**CM.2** The SecurityBaseline Configuration of the information systems shall be documented and updated periodically.

**CM.3** Previous versions of the Security Baseline Configurations shall be retained for rollback.

**CM.4** Organization’s information systems shall be hardened based on established Security Baseline Requirements.

**CM.5** Security Baseline Configuration shall be reviewed and updated based on evolving threats, vulnerabilities, and upgrades to information systems.

**CM.6** The security baseline and hardening configuration tools shall be used to improve the accuracy, consistency, and availability of the Security Baseline Requirements.

**CM.7** Any configured baselines shall be compared with the defined security baselines to identify deviations and take corrective actions.

**CM.8** The information systems configuration changes shall be controlled as per the Change Management Policy.

**CM.9** Configuration items (CIs) shall be uniquely identified and maintained in Configuration Management Database (CMDB).

**CM.10** Logging and monitoring of configuration changes shall be enabled as per the Logging and Monitoring Standard.

**Definitions**

|  |  |
| --- | --- |
| **Definition** | **Description** |
| Baseline Configuration | A documented set of specifications for a system, or a configuration item within a system, that has been formally reviewed and agreed upon at a given point in time, and which can be changed only through change control procedures. |
| Configuration Item | Any item or aggregation of hardware, software, or both, that is designated for configuration management, and is treated as a single entity in the configuration management process. |
| Configuration Database | A database that stores information about Organization's Information Technology (IT) hardware and software components, and the relationships between those components. |
| Hardening | A process intended to eliminate a means of attack by patching vulnerabilities and turning off non-essential services. |
| Information Systems | The 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. |
| Security Baseline Requirements | A recognized, standardized, and established benchmark that stipulates specific secure configuration settings for a given information technology platform. |
| Vulnerability | A weakness in an information system, system security procedures, or internal controls that could be exploited or triggered by a threat source. |

**Acronyms**

|  |  |
| --- | --- |
| **Acronym** | **Description** |
| CI | Configuration Item |
| GCISO | Group Chief Information Security Office |

**References**

* Change Management Policy
* Configuration Management Standard
* Logging and Monitoring Standard
* Configuration Management Procedure

**Revision History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Revision Date** | **Reason for Change** | **Drafted/ Reviewed By** | **Approved By** | **Date Approved** |
| 1.0 | 25th July 2023 | Renamed “Infrastructure Hardening Policy” as “Configuration Management Policy”.  Reviewed and updated the policy as per the ISO 27001:2022 and best practices of NIST 800-53 Rev5. | Jyotisman Chakrabarty | Lakshminarayanan RS | 15th January 2024 |