Wipro’s

Security Patch 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 | December 1, 2003 |

**Purpose**

This policy establishes the security patch management requirements to protect the Organization’s information systems.

**Audience**

Organization’s employees, retainers, contractors, and service providers involved in security patch management.

## Scope

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

**Policy Details**

**SPM.1** The Organization shall continuously monitor the release of applicable security patches.

**SPM.2** Security patch deployment shall be prioritized based on the severity of the identified vulnerabilities.

**SPM.3** Security patch management shall adhere to the Change Management Procedure.

**SPM.4** Security patch deployment method shall be selected as per business requirements.

**SPM.5** Legitimacy of security patch source shall be validated before deployment.

**SPM.6** Planned security patch deployments shall be communicated to the relevant stakeholders.

**SPM.7** Security patches shall be evaluated, tested, and approved before deployment into production.

**SPM.8** A rollback plan shall be prepared and maintained to recover from unsuccessful patch deployments.

**SPM.9** If security patches are unavailable or cannot be deployed, the Organization shall implement compensating security controls as per business requirements.

**SPM.10** The status of security patch deployment shall be published on a periodic basis.

**SPM.11** Logging and monitoring of security patch deployment shall be enabled as per the Logging and Monitoring Standard.

**Definitions**

|  |  |
| --- | --- |
| **Definition** | **Description** |
| Information System | 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. |
| Patch Management | The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs. |
| Vulnerability | A weakness in an information system, system security procedures, or internal controls that could be exploited or triggered by a threat source. |

**References**

* Logging and Monitoring Standard
* Patch Management Procedure
* Change Management Procedure

**Revision History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Revision Date** | **Reason for Change** | **Drafted/ Reviewed By** | **Approved By** | **Date Approved** |
| 1.0 | 14th August 2023 | Reviewed and updated the policy as per the ISO 27001:2022 and best practices of NIST 800-53 Rev5 | Jyotisman Chakrabarty & Sanchay Chakrabarty | Lakshminarayanan RS | 18th January 2024 |