Wipro’s

Malicious Code Protection 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 | June 1, 2007 |

**Purpose**

This policy emphasises the requirement to protect information systems from the risks introduced by malicious code.

## Audience

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

**Scope**

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

**Policy Details**

**MCP.1** The selection and configuration of Malicious Code Protection Solutions shall be determined based on risk assessments and business requirements.

**MCP.2**The Malicious Code Protection Solution shall be configured and implemented on information systems.

**MCP**.**3** The information systems shall be scanned periodically with the latest Malicious Code Protection Solution.

**MCP.4** Email gateways, web security gateways, file-sharing solutions, and other threat vectors shall be configured to detect and prevent malicious code.

**MCP.5** The information systems shall be monitored to detect known or unknown malicious code patterns.

**MCP.6** Software delivered to users and customers shall be free from malicious code.

**MCP.7** Ensure users shall not disable or modify the Malicious Code Protection Solution configurations.

**MCP.8** Malicious code analysis shall be performed using Sandboxing techniques.

**MCP.9** Suspicious malicious code incidents shall be reported, responded to, and remediated as defined in the Security Incident Management Procedure.

**Definitions**

|  |  |
| --- | --- |
| **Definition** | **Description** |
| Malicious Code | A code designed to cause damage, security breaches, or other threats to the information systems security. |
| Organization | Wipro Limited, including subsidiaries, affiliates, and acquired entities, but excluding acquired entities governed by an independent set of security policies. |
| Sandboxing | A technique used to test suspicious programs that may contain viruses or other malicious code. |
| Web Filtering | A technique that screens and blocks access to inappropriate or unsafe web content. |

**References**

* Acceptable Usage Policy
* Internet Access Standard
* Malicious Code Protection Standard
* Malicious Code Protection Procedure
* Security Incident Management Procedure

**Revision History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Revision Date** | **Reason for Change** | **Drafted/ Reviewed By** | **Approved By** | **Date Approved** |
| 1.0 | 25th July 2023 | Reviewed and updated the policy as per the ISO 27001:2022 and best practices of NIST 800-53 Rev5. | Roju Vadakkath | Lakshminarayanan RS | 18th January 2024 |