Wipro’s

Supply Chain Cyber Risk 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 | July 1, 2014 |

**Purpose**

This policy governs the supply chain cyber risk management program and emphasizes the importance to protect the information systems against risks introduced by suppliers.

**Audience**

Organization’s employees, retainers, contractors, service providers, and suppliers engaged in the supply chain risk management program.

**Scope**

This policy applies to suppliers with access to the Organization’s information systems.

**Policy Details**

**SCCM.1** An inventory of the approved suppliers shall be maintained.

**SCCM.2** Suppliers shall be categorized into different tiers based on the potential cyber risk posed to the Organization.

**SCCM.3** Information security risk assessment shall be performed periodically based on the tier, and a report shall be shared with the Business or Function heads.

**SCCM.4** Selection of suppliers shall be based on the information security risk assessment report.

**SCCM.5** The suppliers shall mitigate the identified issues from risk assessments within the agreed timelines.

**SCCM.6** Information security requirements shall be captured as part of the supplier’s contract.

**SCCM.7** Confidentiality, Security and Privacy Addendums, and the Non-Disclosure Agreement (NDA) shall be signed with the suppliers.

**SCCM.8** Supplier information security practices, and changes to supplier services shall be monitored and reviewed.

**Definitions**

|  |  |
| --- | --- |
| **Definition** | **Description** |
| 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. |
| Risk | A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs and the likelihood of occurrence. |
| Supplier | A company or an entity that has a written agreement with the Organization to provide a product, service, or contractors. |
| Supply Chain | Set of resources and processes between and among multiple tiers of Organizations, each of which is an acquirer; this begins with sourcing products and services and extends throughout their lifecycle. |
| Tiering | A process to classify vendors into categories based on the potential cyber risk posed to the Organization. |

## Acronyms

|  |  |
| --- | --- |
| **Acronym** | **Description** |
| GCISO | Group Chief Information Security Office |
| NDA | Non-Disclosure Agreement |

**References**

* Supply Chain Cyber Risk Management Procedure

**Revision History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Revision Date** | **Reason for Change** | **Drafted/ Reviewed By** | Approved By | **Date Approved** |
| 1.0 | 3rd January 2024 | Reviewed and updated the policy as per the ISO 27001:2022 and best practices of NIST 800-53 Rev5. | Harsha Lakkumane | Lakshminarayanan RS | 18th January 2024 |