****

Wipro’s

Insider Threat Management Policy

**Document Control**

|  |  |
| --- | --- |
| Function | Group Chief Information Security Office |
| Sub-function | - |
| Policy Owner | Group Head - Information Security Policy & Framework |
| Policy Effective Date | 22nd July 2024 |

**Purpose**

This policy establishes the requirement to detect, prevent, and respond to Insider Threats to the Organization’s data, information systems, and facilities. The goal is to protect the Organization’s information systems, Intellectual Property, and Sensitive and Confidential Information from unauthorized access, modification, or deletion.

**Audience**

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

**Scope**

This policy applies to all employees, retainers, contractors, and service providers with access to the Organization’s information systems and data.

**Policy Details**

**ITP.1** Periodic risk assessments shall be conducted to identify potential Insider Threats.

**ITP.2** Access to Sensitive Information shall be limited to authorized personnel only, based on their role and need-to-know basis.

**ITP.3** System and user activity monitoring shall be implemented to detect unusual or unauthorized activities.

**ITP.4** Regular training shall be provided to all the stakeholders in-scope on recognizing and reporting potential Insider Threats.

**ITP.5** Policy and its enforcement shall comply with relevant or applicable laws and regulations.

**ITP.6** Employees and other stakeholders in scope shall report any suspicious activity as mentioned in the Security Incident Management Procedure.

**ITP.7** Investigation process of insider threats shall be aligned with Security Incident Management Procedure.

**ITP.8** An Insider Threat Program shall be established and monitored.

**ITP.9** Violation of this policy shall be handled according to the organization’s disciplinary procedures and may result in disciplinary action, including termination of employment or contracts.

**Definitions**

|  |  |
| --- | --- |
| **Definition** | **Description** |
| Confidential Information | Information in any recorded medium that is not available in the public domain comprising or relating to Wipro’s information including but not limited to techniques; schematics; designs; contracts; financial information; sales and marketing plans; business plans; clients; client data; business affairs; operations; strategies; inventions; methodologies; technologies; employees; subcontractors; pricing; service proposals; methods of operations; procedures; products and/or services that an employee may be privy to in the course of employment with Wipro. |
| Insider | Any person with authorized access to any organizational resource, including personnel, facilities, information, equipment, networks, or systems. |
| Intellectual Property | Intellectual Property shall mean patents, industrial designs, copyrights, trademarks, geographical indications, trade secrets, and other legal interests recognized or protected as intellectual property under the governing laws or declared as Intellectual Property. |
| Information Systems | A set of applications, services, information technology assets, or other information handling components. |
| Insider Threat | A risk posed by individuals who have or had authorized access to an organization’s assets and use that access to harm the confidentiality, integrity, or availability of the organization’s data or information systems. |
| Organization | Wipro Limited, including subsidiaries, affiliates, and acquired entities, but excluding acquired entities governed by an independent set of security policies. |
| Sensitive Information | Information, the loss, misuse, or unauthorized access to or modification of, that could adversely affect the organizational interest. |

**Acronyms**

| **Acronym** | **Description** |
| --- | --- |
| BiSM | Business-integrated Security Management |

**References**

* Logging and Monitoring Policy
* Information Access Control Policy
* Acceptable Usage Policy
* User Account Management Policy
* Intellectual Property Policy
* Workplace Monitoring Policy
* Security Incident Management Procedure

**Revision History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Revision Date** | **Reason for Change** | **Drafted/ Reviewed By** | **Approved By** | **Date Approved** |
| 1.0 | 19th June 2024 | New “Insider Threat Management Policy” created. | Legal and Corporate Communications Team | Lakshminarayanan RS | 22nd July 2024 |