Wipro’s

Security Incident 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 | June 1, 2004 |

**Purpose**

This policy governs the Security Incident handling process and incident response lifecycle.

**Audience**

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

**Scope**

This policy applies to information systems and facilities owned or managed by the Organization, its users, customers, and service providers.

This policy is subject to country-specific laws and regulations.

**Policy Details**

**SIM.1** Security Incident Management process shall be defined as per business requirements and shall be communicated to relevant stakeholders.

**SIM.2** The designated team shall detect, analyze, respond to, and recover Security Incidents.

**SIM.3** Security Events shall be reported through appropriate reporting channels as defined in the Security Incident Management Procedure.

**SIM.4** Security Incidents shall be categorized based on severity and impact levels.

**SIM.5** The Legal team shall be consulted based on the complexity and sensitivity of incidents.

**SIM.6** Security Incidents involving loss, exposure, or destruction of regulated information shall be reported to regulators as defined in the Security Incident Management Procedure.

**SIM.7** Security Incidents shall be handled with relevant internal and external stakeholders.

**SIM.8** Post**-**incident analysis shall be performed to identify the root cause of the Security Incident.

**SIM.9** Security Incident report shall be documented and maintained as per the Security Incident Management Procedure.

**SIM.10** Evidence related to Security Incidents shall be identified, collected, and preserved as per the applicable laws, regulations, and business requirements.

**SIM.11** Cyber Security Incident Response Procedure shall be established, reviewed, and tested periodically.

**SIM.12** Lessons learned from Security Incidents shall be leveraged to:

* Enhance the Cyber Security Incident Response Procedure.
* Reduce the likelihood or consequences of similar future incidents.
* Enhance user awareness and training.

**SIM.13** The Organization shall define a strategy to manage public relations while handling Security Incidents.

**SIM.14** The Organization shall establish awareness programs to encourage reporting of Security Incidents.

**SIM.15** Security incident response training shall be provided to relevant users on a periodic basis.

**SIM.16** Security incident analysis reports shall be reviewed by management.

**SIM.17** Logging and monitoring of incident management activities shall be enabled as per the Logging and Monitoring Standard.

**Definitions**

|  |  |
| --- | --- |
| **Definition** | **Description** |
| Security Event | Any event indicating a possible information security breach or failure of controls or violate the security policy of the Information System. |
| Security Incident | A single or a series of unwanted or unexpected security events that have a significant probability of compromising business operations and threatening security. |
| Security Incident Management | A set of processes for detecting, reporting, assessing, responding to, dealing with, and learning from security incidents. |
| Information System | A 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. |

**References**

* Information Security Training and Awareness Standard
* Logging and Monitoring Standard
* Cyber Security Incident Response Procedure
* Security Incident 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. | Roju Vadakkath | Lakshminarayanan RS (LN) | 15th January 2024 |