Wipro’s

Information Security 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, 2009 |

**Purpose**

This policy governs the implementation and management of the Organization’s Information Security Management System (ISMS), which protects information systems from the risks introduced by people, processes, and technology.

**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**

**IS.1** Topic-specific policies, standards, procedures, and guidelines shall support the Information Security Policy.

**IS.2** The ISMS documents shall be defined, approved, published, and communicated within the Organization, and interested parties.

**IS.3** Confidentiality, Integrity, and Availability (CIA) principles shall govern the Organization’s ISMS.

**IS.4** Privacy and accountability of the information shall be maintained as per the laws, regulations, and business requirements.

## IS.5 The Organization shall adhere to the following information security objectives:

**IS.5.1** Define and implement an information security strategy to safeguard the Organization’s information systems.

**IS.5.2** Ensure compliance with applicable laws, regulations, and business requirements.

**IS.5.3** Prevent, detect, and manage information security incidents, breaches, or security violations.

**IS.5.4** Protect the Organization and its customers’ Intellectual Property Rights (IPR).

**IS.5.5** Ensure a business continuity program is planned and implemented to recover business from disruptions.

**IS.5.6** Ensure information security risks related to projects are identified and addressed throughout the project life cycle.

**IS.5.7** Provide information security training and awareness programs periodically to ensure users are aware of the Organization’s information security requirements.

**IS.5.8** Ensure continual improvement of the ISMS through assessments and audits.

**IS.5.9** Identify, assess, mitigate, and monitor information security risks.

**IS.6** The capacity requirements for information processing facilities, human resources, and other facilities shall be identified as per business requirements.

**IS.7** Senior management shall ensure adequate resources are provided to achieve the objectives of the ISMS.

**IS.8** The Designated Team shall plan and conduct the Management Review Meetings (MRM) as defined in the Management Review Meeting (MRM) Procedure.

**IS.9** Information security Organization structure, along with roles and responsibilities, shall be defined in the Security Organization Standard.

**IS.10** The ISMS documents shall be periodically reviewed, updated, approved, and published as per the Information Security Management System Standard.

**IS.11** Exceptions to the ISMS policies shall be handled as per the Exception Handling Procedure.

**IS.12** Employees, retainers, and contractors working at customer locations shall comply with the customer’s Information Security Policy, in addition to Organization’s policies.

**IS.13** Regional or local laws and regulations shall supersede the ISMS policies.

**IS.14** Non-compliance with the ISMS policies shall be subject to disciplinary action.

**Definitions**

|  |  |
| --- | --- |
| **Definition** | **Description** |
| Availability | Information made accessible and usable on demand by authorized individuals, entities, or processes. |
| Business Continuity | The capability of an organization to deliver its products and services at an acceptable and predefined capacity within an acceptable time frame whenever business disruptions occur. |
| Business Requirements | Requirements related to contractors, customer contracts, vendors, and suppliers. |
| Confidentiality | Information that is not made available or disclosed to unauthorized individuals, entities, or processes. |
| Designated Team | A person or team identified and nominated by Senior Management to perform specific duties. |
| Exception | An “exception” is defined as any requirement that deviates from the standard procedures and practices that are set in accordance with the organization’s Information Security Policy. This also includes any special or additional approvals required in addition to the standard practices as defined in the organization’s ISMS. |
| Integrity | Accuracy and completeness of information. |
| Interested Party | A person or organization that can affect, be affected by, or perceive itself to be affected by a decision or activity. |
| Information Security Incident | Single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. |
| Information Security | Preservation of confidentiality, integrity, and availability of information. |
| Information System | Set of applications, services, information technology assets, or other information-handling components. |
| ISMS | A systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organization’s information security to achieve business objectives. |
| ISMS Documents | Set of policies, standards, procedures, and guidelines. |
| Organization | Wipro Limited, including subsidiaries, affiliates, and acquired entities, but excluding acquired entities governed by an independent set of security policies. |
| IPR | Creations of the mind, such as musical, literary, and artistic works; inventions; and symbols, names, images, and designs used in commerce, including copyrights, trademarks, patents, and related rights. Under Intellectual Property Rights law, the holder of one of these abstract “properties” has certain exclusive rights to the creative work, commercial symbol, or invention by which it is covered. |
| Risk | A measure determining the extent of a threat due to a potential circumstance or event, including the magnitude of the harm along with the likelihood of its occurrence. |
| Security | The term “Security” means “Information Security”, across ISMS unless explicitly specified. |
| Threat | An event or situation that has the potential to cause undesirable consequences or impact. |
| User | The term “user” means an employee, retainer, contractor, trainee or intern, customer, partner, and supplier as a baseline definition. Any exception to this definition shall be highlighted in the scope of the respective policies. |
| Vulnerability | A weakness in an information system, system security procedures, or internal controls that could be exploited or triggered by a threat source. |

**Acronyms**

|  |  |
| --- | --- |
| **Acronym** | **Description** |
| CIA | Confidentiality, Integrity, and Availability |
| GCISO | Group Chief Information Security Office |
| ISMS | Information Security Management System |
| IPR | Intellectual Property Rights |
| MRM | Management Review Meetings |
| PII | Personally Identifiable Information |

**References**

* Information Security Management System (ISMS) Standard
* Security Organization Standard
* Disciplinary Action Procedure
* Exception Handling Procedure
* Management Review Meeting (MRM) Procedure

**Revision History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Revision Date** | **Reason for Change** | **Drafted/ Reviewed By** | Approved By | **Date Approved** |
| 1.0 | 5th January 2024 | Merged Information Security Management System Policy, Management Review Policy, and Security Organization Policy.  Reviewed and updated the policy as per the ISO 27001:2022 and best practices of NIST 800-53 Rev5. | Thirunavukkarasu A M | Lakshminarayanan RS | 15th January 2024 |
| 1.0 | 24th June 2024 | No Change | Thirunavukkarasu A M | Lakshminarayanan RS | 24th June 2024 |