Wipro’s

Information Security Management

Systems (ISMS) Audit 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 | January 31, 2012 |

**Purpose**

This policy governs the Organization’s information security audits and assessments program, which ensures compliance with established Information Security Management System (ISMS) policies and drives continual improvements. This policy also supports the Organization in verifying compliance with:

* International Organization for Standardization (ISO) 27001 Standard
* National Institute of Standards and Technology (NIST) 800-53 Special Publication
* Laws and Regulations (Country/Industry)
* Customer contracts and Master Service Agreement (MSA) requirements

**Audience**

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

**Scope**

This policy is applicable across the Organization, including Global Business Lines (GBLs), Strategic Market Units (SMUs), and Functions.

**Policy Details**

**IA.1** The Organization assets, including people, processes, and technologies, shall be audited.

**IA.2** The Organization shall formulate an internal audit function to support and conduct information security internal audits.

**IA.3** Theinternal audit function shall operate independently to ensure impartiality in the audit process.

**IA.4** An internal audit plan shall be prepared, reviewed, and updated based on the perceived risks of information security.

**IA.5** Independent and trained Internal Auditors shall perform internal information security audits.

**IA.6** Internal audits and assessments shall be performed at least annually using manual or automated assessment methods.

**IA.7** The Auditee shall articulate or share the evidence requested by the Internal Auditor.

**IA.8** The Internal Auditor shall report the audit findings to relevant stakeholders.

**IA.9** TheAuditee shall respond with the root cause, correction, corrective actions, and target closure dates.

**IA.10** TheInternal Auditor shall track the closure of the reported audit findings.

**IA.11** Theinternal audit function shall communicate the summary of audit findings to the business and/or function heads.

**Definitions**

|  |  |
| --- | --- |
| **Definition** | **Description** |
| Assets | Anything that has value to the Organization which includes the information assets, software assets, physical assets, virtual assets, services assets, people assets, and IoT assets. |
| Auditee | An Auditee is a person or an Organization that is being audited. |
| ISMS | An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Organization’s information security to achieve business objectives. |
| Information resources | It refers to the information and related resources, such as personnel, equipment, and information technology. |
| Internal audit function | An Internal audit function represents one or more auditors responsible for jointly evaluating the information security systems and processes. |
| Internal Auditor | An Internal Auditor is a trained professional who provides independent and objective evaluations of information security systems or processes. |
| Organization | Wipro Limited, including subsidiaries, affiliates, and acquired entities, but excluding acquired entities governed by an independent set of security policies. |

**Acronyms**

|  |  |
| --- | --- |
| **Acronym** | **Description** |
| GBL | Global Business Lines |
| GCISO | Group Chief Information Security Office |
| ISMS | Information Security Management System |
| ISO | International Organization for Standardization |
| MSA | Master Service Agreement |
| NIST | National Institute of Standards and Technology |
| SMU | Strategic Market Units |

**References**

* Information Security Policy
* Information Security Management Systems (ISMS) Audit Procedure

**Revision History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Revision Date** | **Reason for Change** | **Drafted/ Reviewed By** | **Approved By** | **Date Approved** |
| 1.0 | 27th June 2023 | Reviewed and updated the policy as per the ISO 27001:2022 and best practices of NIST 800-53 Rev5. | Venkateshwaran R | Lakshminarayanan RS | 15th January 2024 |
| 1.1 | 28th May 2024 | Updated frequency in IA.6 point. | Venkateshwaran R | Lakshminarayanan RS | 28th May 2024 |