

Wipro’s Information Security Training and

Awareness 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 establishes the need to provide personnel with training to create awareness of their responsibilities in protecting the Organization’s information.

**Audience**

Organization’s employees, retainers, and contractors.

**Scope**

This policy applies to personnel who have access to Organization’s information systems.

**Policy Details**

**STA.1** The Information Security Training team shall develop and deliver the Information Security Training and Awareness Program.

**STA.2** The Information Security Training and Awareness Program shall be updated in accordance with applicable laws, regulations, business requirements, and evolving threats.

**STA.3** The Information Security Training shall be provided to personnel while they join the Organization as part of their induction.

**STA.4** The Information Security Annual Refresher Training shall be completed within timelines.

**STA.5** Personnel shall undergo Information Security Training, as well as read and acknowledge the Organization’s Information Security Management System (ISMS) policies periodically.

**STA.6** Role-based Information Security Training shall be provided based on the employee’s job responsibilities.

**STA.7** Personnel working at customer locations shall comply with customer-specific Information Security Training and Awareness requirements.

**STA.8** The Information Security Training team shall communicate ISMS changes to personnel.

**STA.9** Periodic phishing simulation exercises shall be conducted as per business requirements. Personnel failing to identify simulated phishing emails shall undergo a refresher course on phishing awareness.

**STA.10** Information Security Training and Awareness Program records shall be retained as per the Data Retention Policy.

**STA.11** Information Security Training Program feedback shall be collected and analyzed to identify improvement areas.

**STA.12** Regional or local laws and regulations shall supersede this policy.

**Definitions**

|  |  |
| --- | --- |
| **Definition** | **Description** |
| ISMS | A systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Organization’s information security to achieve business objectives. |
| Information Security Training and Awareness Program | A program with a set of activities designed to plan, deliver, monitor, and improve Information Security Training and Awareness within the Organization. |
| 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. |
| Personnel | Persons working under the Organization’s direction. |
| Phishing | A process of attempting to acquire sensitive information, such as usernames, passwords, and personal information, by impersonating a trustworthy entity or user by sending emails to persuade the users either to click on a link or download a malicious attachment. |
| Simulation exercise | A real-time exercise designed to simulate the learning experience of personnel and evaluate their ability to respond to information security incidents in a timely and effective manner. |

**Acronyms**

|  |  |
| --- | --- |
| **Acronym** | **Description** |
| GCISO | Group Chief Information Security Office |
| ISMS | Information Security Management System |

**References**

* Data Retention Policy
* Personnel Security Policy
* Information Security Training and Awareness Standard

**Revision History**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version** | **Revision Date** | **Reason for Change** | **Drafted/ Reviewed By** | **Approved By** | **Date Approved** |
| 1.0 | 19th July 2023 | Reviewed and updated the policy as per the ISO 27001:2022 and best practices of NIST 800-53 Rev5 | Ramesh Babu Mundayat | Lakshminarayanan RS | 15th January 2024 |
| 1.0 | 4th June 2024 | No Change | Ramesh Babu Mundayat | Lakshminarayanan RS | 4th June 2024 |