Wipro’s

Personnel 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 | December 1, 2003 |

**Purpose**

This policy establishes personnel security requirements to comply with the Organization’s information security posture.

**Audience**

Organization’s employees, retainers, contractors, trainees or interns, and service providers.

**Scope**

This policy applies to employees, retainers, contractors, and trainees or interns having access to the Organization’s information.

**Policy Details**

**PS.1** Background verification checks shall be conducted prior to authorizing access to the information systems.

**PS.2** Background verification checks shall be conducted as per the screening criteria derived from applicable laws, regulations, business requirements, and customer-specific requirements.

**PS.3** Employees, retainers, contractors, trainees or interns, and suppliers shall sign a confidentiality or Non-Disclosure Agreement (NDA).

**PS.4** The terms and conditions of employment, contract, or agreement shall contain the information security requirements that are valid during and after the termination or change of employment.

**PS.5** Roles and responsibilities for information security shall be incorporated into organizational job descriptions and communicated accordingly.

**PS.6** Employees, retainers, and contractors shall comply with the Organization’s information security policies and any breaches/security lapses shall be handled as per the disciplinary policy. All employees, retainers, and contractors shall undergo mandatory security awareness and training.

**PS.7** Employees, retainers, and contractors working in customer locations shall comply with the customer-specific information security policies in addition to Organization’s policies.

**PS.8** Any information security incidents, suspicious activities, and policy violations shall be reported via the following:

* Wipro Limited Users: **The Dot >> Apps >> WiServe >> Security Incident Report >> Report a Security Incident (SIR)**
* Wipro DOP Users: **The Dot >> Apps >> Business Applications >> RMAC SIR**.

**PS.9** Resigned or terminated employees, retainers, and contractors shall acknowledge the post-employment information security requirements.

**PS.10** Exit interviews shall be conducted for the resigned or terminated employees, retainers, and contractors.

**Definitions**

|  |  |
| --- | --- |
| **Definition** | **Description** |
| 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 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 doing work under the Organization’s direction. |

#### Acronyms

|  |  |
| --- | --- |
| **Acronym** | **Description** |
| GCISO | Group Chief Information Security Office |
| NDA | Non-Disclosure Agreement |

**References**

* Information Security Training and Awareness Policy
* Security Incident Management Policy
* Supply Chain Cyber Risk Management Policy
* Information Security Policy
* Personnel Security Standard

## 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. | Thirunavukkarasu A M | Lakshminarayanan RS | 18th January 2024 |