Wipro’s

Workplace Monitoring 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, 2014 |

**Purpose**

This policy establishes the requirement of workplace monitoring to ensure compliance with legal or contractual obligations.

**Audience**

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

**Scope**

This policy applies to information systems, assets and facilities owned and managed by the Organization.

**Policy Details**

**WMP.1** The Organization shall monitor information systems usage as per the Acceptable Usage Policy and the Data Protection and Privacy Policy.

**WMP.2** Personnel shall comply with the contract of employment and Organization policies, including the Code of Business Conduct (COBC).

**WMP.3** Users shall be made aware if the tracking and monitoring of information systems may reveal their Personally Identifiable Information (PII), as per applicable local data privacy requirements.

**WMP.4** The Organization shall reserve the right to monitor and detect physical impersonation, password sharing, data downloads, and timesheet mismatches.

**WMP.5** E-mail message filtering shall be performed to monitor e-mail messages.

**WMP.6** Access to monitoring applications and reports shall be granted to designated personnel based on the business requirements.

**WMP.7** Suspicious usage of the information system shall be reported and remediated as per the Security Incident Management Procedure.

**Definitions**

|  |  |
| --- | --- |
| **Definition** | **Description** |
| Asset | 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. |
| Designated Personnel | A person identified and nominated by the Senior Management to perform specific duties. |
| Information Systems | Set of applications, services, information technology assets, or other information-handling components. |
| E-mail Filters | Software or hardware-based mechanisms that analyze the incoming and outgoing emails and apply predefined rules to determine whether an email should be allowed through, flagged as suspicious, or blocked altogether. |
| Physical Impersonation | A social engineering tactic, where an individual pretends to be someone else in a physical or face-to-face setting to gain unauthorized access to a restricted area, sensitive information, or valuable assets. |
| Monitoring Applications | Software or tools that are used to monitor and collect data from various sources within an Organization’s IT infrastructure. |
| Organization | Wipro Limited, including subsidiaries, affiliates, and acquired entities, but excluding acquired entities governed by an independent set of security policies. |
| Personally Identifiable Information (PII) | Information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual. |

**Acronyms**

|  |  |
| --- | --- |
| **Acronym** | **Description** |
| COBC | Code of Business Conduct |
| GCISO | Group Chief Information Security Office |
| PII | Personally Identifiable Information |

**Reference**

* Data Protection and Privacy Policy (Personally Identifiable Information)
* Acceptable Usage Policy
* Information Security Policy
* 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. | Rajiv Singh Johri | Lakshminarayanan RS | 18th January 2024 |
| 1.0 | 31st May 2024 | No Change | Rajiv Singh Johri | Lakshminarayanan RS | 31st May 2024 |