Wipro’s

Network 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 | March 1, 2022 |

**Purpose**

This policy establishes the network security requirements to protect the Organization’s information systems.

**Audience**

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

**Scope**

This policy applies to the Organization’s network and network devices including network connectivity with customers, suppliers and third-party vendors.

**Policy Details**

**NSP.1** Inventory of the network and the network devices shall be maintained and reviewed.

**NSP.2** The network and network devices shall be configured as per the Configuration Management Policy.

**NSP.3** Access to the network devices shall be granted through secure login methods, including strong passwords and Multi-Factor Authentication (MFA).

**NSP.4** Anyunauthorized access to the network and the network devices shall be restricted.

**NSP.5** Access to the network and the network devices shall be reviewed periodically.

**NSP.6** The data in transit over the network shall be encrypted as per the Encryption Policy.

**NSP.7** Network segmentation shall be implemented, and traffic flow shall be protected through an access control mechanism.

**NSP.8** The network devices shall be synchronized as per the Clock Synchronization Standard.

**NSP.9** Redundancy of the network and the network devices shall be based on business requirements.

**NSP.10** The network of supporting utilities shall be segregated from the Information Technology (IT) network.

**NSP.11** The vulnerability and risk assessments shall be performed on the network devices prior to production deployment and on a periodic basis.

**NSP.12** Logging and Monitoring of the network and the network devices shall be enabled.

**NSP.13** Suspicious activities and security breaches related to the network and the network devices shall be reported and remediated.

**Definitions**

|  |  |
| --- | --- |
| Definition | **Description** |
| Authentication | Verifying the identity of a user, process, or device while allowing access to information systems. |
| Authorization | Access privileges granted to a user, program, or process, or the act of granting those privileges. |
| Encryption | The process of changing plaintext into ciphertext using a cryptographic algorithm and key. |
| Information Systems | Set of applications, services, information technology assets, or other information-handling components. |
| Network | An information system implemented with a collection of interconnected components such as computers, routers, switches, hubs, cabling, and telecommunications controllers. |
| Organization | Wipro Limited, including subsidiaries, affiliates, and acquired entities, but excluding acquired entities governed by an independent set of security policies. |
| Supporting utilities | The equipment or devices used for operations and management of facilities (electricity, water supply, gas, sewage, ventilation, and air conditioning) supporting information processing. |
| Vulnerability | A weakness in a system, application, or network that is subject to exploitation or misuse. |

**Acronyms**

|  |  |
| --- | --- |
| **Acronym** | Description |
| GCISO | Group Chief Information Security Office |
| IT | Information Technology |
| MFA | Multi-Factor Authentication |

**References**

* Asset Management Policy
* Configuration Management Policy
* Encryption Policy
* Information Security Continuity Policy
* Clock Synchronization Standard
* Logging and Monitoring Standard
* Network Security Standard
* Password Management Standard
* Security Incident Management Procedure
* Network Security 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. | Ravi Baniwal | Lakshminarayanan RS | 18th January 2024 |