Wipro’s

Remote Access 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 | February 1, 2003 |

**Purpose**

This policy governs the remote access to the Organization’s information systems and protects it against the risks introduced by the remote users and any unauthorized access.

**Audience**

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

## Scope

This policy applies to the Organization’s information systems that are accessible remotely.

**Policy Details**

**RA.1** Remote access shall be provided from managed, unmanaged, and mobile devices using the approved remote access methods.

**RA.2** Remote access shall be provided to employees, retainers, and contractors, based on the principle of least privilege and as per business requirements.

**RA.3** Privileged remote access to information systems shall be authorized by the asset owner as per business requirements.

**RA.4** Remote access to perform administrative, maintenance, and diagnostic activities shall be approved by the asset owner.

**RA.5** Remote access services shall be permitted over private network as well as public network by using secured encryption protocols.

**RA.6** Remote access from managed devices shall comply with configuration and security requirements as defined in the Remote Access Standard.

**RA.7** Remote access from unmanaged devices shall comply with configuration and security requirements as defined in the Third-Party Access Standard.

**RA.8** Mobile devices shall be enrolled in Mobile Device Management (MDM) application to access the Organization’s information.

**RA.9** Remote access to information systems through personal devices shall be allowed with necessary approvals.

**RA.10 Users shall adhere to the following requirements:**

**RA.10.1** Complete the mandatory information security training and awareness modules as per the Information Security Training and Awareness Policy.

**RA.10.2** Devices shall not be left unattended.

**RA.10.3** Ensure that devices shall not be accessed by unauthorized personnel, including family members, friends, and visitors.

**RA.10.4** Report lost or stolen devices to the Information Technology (IT) helpdesk.

**RA.10.5** Report unauthorized remote access attempts or suspicious activities 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**.

**RA.11** Remote access privileges shall be revoked upon the termination of employment, contract, or when access is no longer required.

**RA.12** Logging and monitoring of remote access connections shall be enabled as per the Logging and Monitoring Standard.

**Definitions**

|  |  |
| --- | --- |
| **Definition** | **Description** |
| Data in Transit | Data transferred between locations over a private network or the internet. |
| Encryption | The process of changing plain text into cipher text using a cryptographic algorithm and key. |
| Information Systems | Set of applications, services, information technology assets, or other information-handling components. |
| Logging | Logging refers to keeping a record of the events occurring within the Organization's systems and network. |
| Managed Devices | Devices that are managed by the Organization and the compliance of these devices are aligned with the Organization’s information security control requirements. |
| Organization | Wipro Limited, including subsidiaries, affiliates, and acquired entities, but excluding acquired entities governed by an independent set of security policies. |
| Remote Access | Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network. |
| Unmanaged Devices | Devices that are not managed by the Organization. |

**Acronyms**

|  |  |
| --- | --- |
| **Acronym** | Description |
| GCISO | Group Chief Information Security Office |
| IT | Information Technology |
| MDM | Mobile Device Management |

**References**

* Information Security Training and Awareness Policy
* Network Security Policy
* Logging and Monitoring Standard
* Remote Access Standard
* Third Party Access 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 | Ravi Baniwal | Lakshminarayanan RS | 18th January 2024 |