Wipro’s

Cloud 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 | July 1, 2022 |

**Purpose**

This policy governs the security of Organization’s Cloud Information Systems.

**Audience**

Wipro’s employees, retainers, contractors, and service providers, who are using and managing cloud information systems.

**Scope**

This policy applies to the Cloud Information Systems owned or managed by the Organization.

**Policy Details**

**CSP.1** Information security risk assessments are conducted to assess Cloud Services usage.

**CSP.2** The Organization shall obtain information security assurance certificates or reports from Cloud Service Providers (CSP) as per business requirements.

**CSP.3** The Organization shall have necessary Cloud Service agreements with the CSP.

**CSP.4** Cloud Information Systems shall be hardened as per the Configuration Management Standard.

**CSP.5** Access to Cloud Information Systems shall be granted as defined in the User Account Management Standard.

**CSP.6** The Organization’s cloud data shall be encrypted as per the Encryption Policy.

**CSP.7** Cloud data backup shall be performed as per business requirements.

**CSP.8** Business Continuity Plan (BCP) and Disaster Recovery (DR) Plan shall be created and maintained as per business requirements.

**CSP.9** Changes to the Cloud Information Systems shall be implemented as per the Change Management Procedure.

**CSP.10** Cloud Services usage shall be reviewed periodically to manage information security risks.

**CSP.11** Cloud security internal audits shall be performed periodically.

**CSP.12** Security incidents related to inappropriate usage of the Cloud Services shall be reported as per the Security Incident Management Procedure.

**CSP.13** Cloud Information Systems shall be securely managed and disposed of as per applicable laws, regulations, and business requirements.

**CSP.14** Logging and monitoring of the Cloud Services shall be enabled as per the Logging and Monitoring Standard.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Definitions**   |  |  | | --- | --- | | Definition | **Description** | | BCP | The process involved in creating a system of prevention and recovery against potential threats to Wipro. The plan ensures that personnel and assets are protected and can function quickly in the event of a disaster. | | Cloud Information System | Set of applications, services, information technology assets, or other information-handling components hosted on Cloud. | | CSP | A service provider offering a cloud-based platform, infrastructure, application, or storage services. | | DR | A set of policies, tools, and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster. | | Information System | A set of applications, services, information technology assets, or other information-handling components. | | Encryption | The process of changing plaintext into ciphertext using a cryptographic algorithm and key. | | Organization | Wipro Limited, including subsidiaries, affiliates, and acquired entities, but excluding acquired entities governed by an independent set of security policies. |   **Acronyms**   |  |  | | --- | --- | | **Acronym** | Description | | BCP | Business Continuity Plan | | CSP | Cloud Service Provider | | DR | Disaster Recovery | | GCISO | Group Chief Information Security Office | | ISMS | Information Security Management System |   **References**   * Encryption Policy * Supply Chain Cyber Risk Management Policy * Configuration Management Standard * User Account Management Standard * Cloud Security Standard * Logging and Monitoring Standard * Change Management Procedure * Security Incident Management Procedure * Information Security Management Systems (ISMS) Audit Procedure * Cloud Security Guidelines |

**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. | Harish Arulkumar & Prasanth Muralidharan | Lakshminarayanan RS | 17th January 2024 |