Wipro’s

Information Access Control 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 | October 16, 2018 |

**Purpose**

This policy establishes the requirement for provisioning and managing user accounts and user privileges to access organization’s information systems.

**Audience**

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

**Scope**

This policy applies to generic, privileged, service, break glass, and guest user accounts owned or managed by the organization.

**Policy Details**

**IAC.1 User Account Management**

**IAC.1.1** Information provided for user account creation and deletion shall be verified by the designated personnel.

**IAC.1.2** **Generic accounts, privileged accounts,** service accounts, break glass accounts, and guest accounts with required privileges shall be created, approved, and managed as per business requirements.

**IAC.1.3** User accounts shall be unique and identifiable with the account owner, and passwords shall be created as per the Acceptable Usage Policy.

**IAC.1.4** Assigned user access privileges shall be used for business purposes.

**IAC.1.5** User’saccess to information systems shall be authenticated and authorized.

**IAC.1.6** **Privileged and service** accounts shall be onboarded and managed through the **Privileged Access Management (**PAM) solution.

**IAC.1.7** User accounts, p**rivileged accounts, generic accounts, service** accounts, break glass accounts, and guest accounts shall be reviewed and reconciled by the designated personnel, as per the periodicity defined in the User Account Management Standard.

**IAC.1.8** Dormant and orphan user accounts shall be revoked based on the access reviews.

**IAC.1.9** User accounts and privileged accounts shall be revoked on the user’s separation or termination.

**IAC.1.10** Information system owner shall notify the designated personnel when a service account is no longer required, or if the service is decommissioned.

**IAC.2 Information Access Control**

**IAC.2.1** Access to information systems shall be granted based on the principle of least privilege.

**IAC.2.2** Access to information systems shall be authorized by the designated personnel.

**IAC.2.3** Access to information systems shall be managed through secure login methods.

**IAC.2.4** Access rights to information systems shall be reviewed periodically by the designated personnel.

**IAC.2.5** Privileged access shall be managed through the Privilege Access Management (PAM).

**IAC.2.6** Role-based access controls shall be implemented to ensure segregation of duties.

**IAC.2.7** Access controls shall be implemented as per the applicable regulations and business requirements.

**IAC.3** Security incidents related to the violation of information systems access rights shall be reported as per the Security Incident Management Procedure.

**IAC.4** Logging and monitoring information systems access shall be enabled as per the Logging and Monitoring Standard.

**Definitions**

|  |  |
| --- | --- |
| **Definition** | **Description** |
| Designated Personnel | A person identified and nominated by the senior management to perform specific duties. |
| Break Glass Accounts | Accounts that can be used only in case of an emergency or system outage that prevents normal access to systems. |
| Dormant Accounts | Accounts of users in service that have not been used for a defined period. |
| 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. |
| Orphan Accounts | Active account of a user without ownership or custodian in Global Address List or system. |
| Privileged Accounts | Accounts assigned to individual users that have elevated privileges. |
| Service Accounts | Accounts used by applications or services and do not have interactive login. |
| Users | The term “User” includes employee of the Organization, retainers, contractors, trainees or interns, customers, partners, suppliers, and vendors. |
| User Account Management | Activities involving user identification, account creation, modification, deletion, and access review. |
| User Accounts | Unique accounts assigned to individual users for standard usage. |

**Acronyms**

|  |  |
| --- | --- |
| **Acronym** | **Description** |
| GCISO | Group Chief Information Security Office |
| **PAM** | **Privileged Access Management** |

**References**

* Acceptable Usage Policy
* Information Access Control Standard
* Logging and Monitoring Standard
* User Account Management Standard
* 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. | Jaydeep Jadhav | Lakshminarayanan RS | 15th January 2024 |