Identity Management Policy

Purpose and Scope

1.1 Purpose

This policy establishes the formal procedures for managing the **lifecycle of all user accounts** (creation, modification, enablement, disablement, and removal) to ensure that only **authorized users** have appropriate access to internal systems and applications, especially those that interact with **sensitive data** (e.g., client data, personal data).

1.2 Scope

This policy applies to the management of all user and system accounts across all organizational networks and information systems, and to all personnel (employees, contractors, vendors) responsible for managing or utilizing these accounts.

2. Account Authorization and Creation

2.1 Account Specification and Authorization

The organization must formally **specify and document** the following for all information systems:

- **Authorized Users:** A list or group defining individuals permitted to use the system.
- **Group and Role Membership:** Clearly defined groups and roles (e.g., "HR Manager," "System Auditor") and the specific permissions associated with each.
- **Access Authorizations:** The level of access (e.g., Read, Write, Admin) granted to each role or group.

2.2 Approval Process for Account Creation

All requests for the creation of new information system accounts must be approved by the **Information Owner** or the delegated manager of the system/data. This ensures that a business justification and knowledge of the data's sensitivity support the request.

2.3 Adherence to Access Control Policy

All processes for creating, enabling, modifying, disabling, and removing information system accounts **must be conducted in strict accordance with the Access Control Policy** and its defined workflow.

3. Account Privilege and Access Control

3.1 Consideration of Segregation of Duties (SoD)

When allocating user access permissions, **Segregation of of Duties (SoD) must be considered and enforced**. No single user should be granted conflicting permissions that would allow them to control an entire critical business process, such as the ability to both initiate and approve financial transactions. User roles and group memberships must be designed to prevent SoD violations.

3.2 Access Modification

Any modifications to a user's account permissions (e.g., role changes, temporary privileged access) must follow the formal **access approval process** defined in the Access Control Policy, ensuring approval by the appropriate manager or **Information Owner**.

4. Account Disablement and Removal

4.1 Account Disablement for Departed Users

User IDs for personnel who have left the organization (whether voluntary or involuntary termination) must be **immediately disabled or removed** upon notification from the Human Resources (HR) or management department.

4.2 Account Removal/Decommissioning

Disabled accounts must be **removed from the system** (decommissioned) after a quarantine period of **90 days**, unless a longer period is legally or forensically required. Account removal must be logged and verified.

4.3 Redundant User ID Prohibition

Redundant (removed) user IDs shall not be reallocated to alternative or new users. A new user must always be assigned a unique User ID to maintain non-repudiation and an accurate audit trail.

5. Account Auditing and Review

5.1 Periodic Reviews for Dormant/Redundant Accounts

Periodic reviews must be conducted at least **quarterly** to proactively identify **dormant or redundant user IDs**. A dormant account is defined as any account that has not been used or logged into for **90 consecutive days**.

5.2 Dormant Account Management

Identified dormant accounts must be immediately **disabled** and investigated. If no business justification for the dormancy is provided and approved by the Information Owner within 30 days, the account will be **removed** in accordance with Section 4.2.

5.3 Review Records

Records of all account reviews, including the justification for keeping any accounts that appear dormant, must be maintained for audit purposes.