Popular Vehicles
& Services

Policy Related to Information Technology Security

ACCESS CONTROL & IDENTITY MANAGEMENT POLICY

Document Title : Access Control & Identity Management Policy

Version : 1.0

Effective Date : 31-01-2026

Review Cycle : Annual

Policy Owner : IT / Information Security

Approval Authority : Management / Board of Directors

1. Purpose

The purpose of this policy is to define controls for user access management to ensure that access to information systems and data is authorized, appropriate, and traceable throughout the user lifecycle. This policy supports the principles of least privilege, accountability, and compliance with Information Security and Information Systems (IS) audit requirements.

2. Scope

This policy applies to all employees, contractors, consultants, and authorized third parties who access organizational information systems. It covers all information assets and environments, including applications, databases, servers, endpoints, network infrastructure, and cloud platforms, whether hosted on-premises or externally.

3.Access Control Principles

The organization shall:

- Grant access to information systems and data **strictly based on business requirements and defined job roles,** ensuring users have access only to what is necessary to perform their duties
- Apply the **principle of least privilege** to limit access rights and reduce the risk of unauthorized or excessive access
- Ensure that all user access is **formally approved, periodically reviewed, and promptly modified or revoked** in response to role changes, transfers, or termination
- Maintain **accurate and complete access records,** including access approvals, modifications, and removals, to support accountability, monitoring, and audit requirements
-

4. Roles and Responsibilities

Management / Business Owners

- Approve user access requests based on business requirements and job responsibilities
- Ensure access provided to users remains appropriate through periodic access reviews
- Support timely removal or modification of access when roles change or employment ends.

IT / Information Security

- Provision, modify, and de-provision user access in accordance with approved requests
- Implement and enforce access control mechanisms and security controls
- Maintain access management records and audit evidence, including approvals, reviews, and removals
- Monitor access-related events and support audit and compliance activities

Users

- Use granted access solely for authorized business purposes
- Protect assigned credentials and access privileges from unauthorized use
- Promptly report any access-related issues, misuse, or suspected security incidents

Policy Statements

User Provisioning

- User access shall be provisioned only upon **formal approval** from authorized management or system owners
- Access granted shall align with the user's assigned role and documented business requirements

User De-Provisioning

- User access shall be **promptly revoked** upon employee exit, contract termination, or loss of business need
- Evidence of access removal shall be maintained for audit purposes

Role-Based Access Control (RBAC)

- Access rights shall be assigned based on **predefined roles** aligned with job functions
- Role definitions shall be reviewed periodically to ensure continued relevance and appropriateness

Privileged Access

- Administrative and privileged access shall be **restricted to authorized personnel** only
- Privileged access shall require management approval and be subject to additional controls and monitoring
- Privileged accounts shall be used solely for administrative activities

Joiner / Mover / Leaver (JML) Process

- **Joiners:** Access shall be provided based on approved role and business requirements
- **Movers:** Access shall be reviewed and updated when users change roles or responsibilities
- **Leavers:** All system access shall be revoked immediately upon separation from the organization

Periodic Access Review

- User access rights shall be reviewed **periodically** to confirm alignment with current roles and responsibilities
- Any unauthorized, excessive, or obsolete access identified during reviews shall be removed in a timely manner

---

6. Audit and Evidence

The following evidence shall be maintained:

- Access request and approval records

- Role assignment documentation

- Access review records

- Terminated user access removal proof

- Privileged access approvals

7. Compliance

Non-compliance may result in disciplinary action.

8. Review

This policy shall be reviewed annually.

9. Approval

This policy has been reviewed and approved by the following authorities:

Role	Name	Signature	Date
Board of Directors / Management			
Head – IT			