Popular Vehicles & Services

Policy Related to Information Technology Security

CLOUD SECURITY & USAGE POLICY

Document Title : Cloud Security & Usage 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 establish requirements for the secure use, management, and governance of cloud services to protect organizational information assets. This policy ensures that cloud environments are used responsibly, securely, and in alignment with Information Security objectives and Information Systems (IS) audit requirements.

---

2. Scope

This policy applies to all employees, contractors, consultants, and authorized third parties. It covers all cloud platforms, services, and resources used by the organization, including public, private, and hybrid cloud environments, and cloud-based infrastructure, platforms, applications, and data.

---

3. Cloud Security Principles

The organization shall:

Use cloud services only for authorized business purposes

Protect cloud resources against unauthorized access, data loss, and misconfiguration

Apply the principle of least privilege to cloud access

Ensure visibility, logging, and accountability within cloud environments

---

4. Cloud Usage

Cloud services shall be used only after appropriate authorization

Access to cloud resources shall be through approved identities and authentication mechanisms

Use of unapproved cloud services for business data is prohibited

5. Access Control and Authentication

Access to cloud environments shall be role-based and need-to-know

Administrative and privileged access shall be restricted and controlled

Multi-factor authentication (MFA) shall be enforced for cloud administrative access and remote access where applicable

6. Data Protection in the Cloud

Organizational data stored or processed in cloud environments shall be protected in accordance with the Data Protection Policy

Sensitive and confidential data shall be stored only in approved cloud services

Appropriate security controls shall be applied to prevent unauthorized access or data leakage

7. Logging and Monitoring

Logging shall be enabled for cloud systems and services to record user activities, access events, and administrative actions

Cloud logs shall be protected, retained, and reviewed in accordance with the Logging, Monitoring & Audit Trail Policy

8. Cloud Configuration and Security Controls

Cloud resources shall be configured securely using approved standards and guidelines

Security configurations shall be reviewed periodically to identify misconfigurations or risks

Unused or unnecessary cloud resources shall be reviewed and removed where appropriate

9. Roles and Responsibilities

IT / Information Security:

Govern and manage cloud security controls

Monitor cloud usage and security events

Maintain audit evidence related to cloud security

Management / System Owners:

Approve cloud usage for business purposes

Ensure cloud services meet business and security requirements

Users:

Use cloud services responsibly and in accordance with organizational policies

Protect cloud access credentials and report security incidents promptly

---

10. Audit and Evidence

Audit evidence shall include cloud access control settings, MFA enforcement proof, cloud logging configurations, usage approval records, and evidence of security reviews or corrective actions.

---

11. Compliance

Compliance with this policy is mandatory. Non-compliance may result in disciplinary action in accordance with organizational policies and applicable laws.

---

12. Review

This policy shall be reviewed annually or upon significant changes to cloud services, technology, or regulatory requirements.

---

13. Approval

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

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