Popular Vehicles & Services

Policy Related to Information Technology Security

INFORMATION SECURITY POLICY

Document Title: Information Security 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

This policy establishes the organization's commitment to safeguarding the confidentiality, integrity, and availability of information assets. It provides a high-level framework for information security governance and supports for Information Systems requirements.

2. Scope

This policy applies to all employees, contractors, consultants, and authorized third parties, and covers all organizational information assets, including systems, applications, data, networks, infrastructure, and cloud-based services, whether on-premises or hosted.

3. Information Security Principles

The organization shall:

- Safeguard information against unauthorized access, disclosure, modification, or destruction
- Maintain availability and reliability of information systems to support business operations
- Apply appropriate security controls based on risk assessment and business impact
- Ensure compliance with applicable legal, regulatory, contractual, and audit requirements

4. Governance and Responsibilities

Board of Directors

- Approves the Information Security Policy
- Provides oversight of information security governance and risk

Management

- Ensures implementation and enforcement of this policy
- Allocates appropriate resources to support information security

IT / Information Security

- Implements and maintains security controls
- Monitors systems, logs, and security events
- Responds to and manages security incidents

Users

- Comply with this policy and related procedures
- Protect assigned credentials and access
- Promptly report suspected or actual security incidents

5. Policy Statements

Access Control:

Access to information systems and data shall be granted based on role-based and need-to-know principles. User access rights shall be reviewed periodically and promptly modified or revoked upon role change, transfer, or exit.

Authentication:

Strong authentication mechanisms, including multi-factor authentication (MFA), shall be enforced for critical systems, privileged accounts, and remote access to reduce the risk of unauthorized access.

Logging and Monitoring:

System, application, and security logs shall be enabled, protected from unauthorized modification, and retained for a defined period to support security monitoring, incident investigation, and audit requirements.

Data Protection:
Information shall be classified and handled in accordance with its sensitivity and business impact. Unauthorized access, use, disclosure, or sharing of information is strictly prohibited.

Backup and Recovery:

Critical systems and data shall be backed up regularly and recovery capabilities shall be maintained to support business continuity and operational requirements.

Incident Reporting:

Security incidents shall be reported promptly, investigated in a timely manner, and managed in accordance with established incident response processes.

Cloud Security:
Cloud services and resources shall be configured and managed securely in accordance with organizational security requirements. Access to cloud environments shall follow the principles of least privilege, and cloud assets shall be protected against unauthorized access, data loss, and misconfiguration

6. Compliance

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

7. Review

This policy shall be reviewed at least annually, or earlier in the event of significant changes to business, technology, or regulatory requirements.

8. Approval

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

Role	Name	Signature	Date
Board of Directors			
Head – IT			