Popular Vehicles & Services

Policy Related to Information Technology Security

DATA PROTECTION POLICY

Document Title : Data Protection Policy

Version : 1.0

Effective Date :

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 protection of organizational data to ensure its confidentiality, integrity, and availability. This policy aims to prevent unauthorized access, use, disclosure, alteration, or loss of data and supports Information Security governance and Information Systems (IS) audit requirements.

2. Scope

This policy applies to all employees, contractors, consultants, and authorized third parties. It covers all organizational data, including business, customer, employee, and system data, in electronic, physical, and verbal form, across on-premises, cloud, and hybrid environments.

3. Data Protection Principles

The organization shall:

- Protect data based on its sensitivity and business impact

- Prevent unauthorized access, disclosure, modification, or destruction of data

- Ensure data is accessed and used only for authorized business purposes

- Apply appropriate controls throughout the data lifecycle, from creation to disposal

4. Data Classification

- Organizational data shall be classified based on sensitivity and criticality

- Data classification shall guide handling, access, storage, and protection requirements

- Users shall handle data in accordance with its assigned classification

5. Data Handling and Access

- Access to data shall be granted on a need-to-know and role-based basis

- Data shall be stored and transmitted using approved systems and security controls

- Unauthorized copying, sharing, or disclosure of data is strictly prohibited

- Sensitive data shall not be stored on unauthorized devices or locations

6. Data Sharing and Transfer

- Data sharing with internal or external parties shall be permitted only for legitimate business purposes

- Appropriate approvals and safeguards shall be in place before sharing sensitive or confidential data

- Secure and approved methods shall be used for data transfer

7. Data Retention and Disposal

- Data shall be retained only for the period required to meet business, legal, regulatory, and audit requirements

- Data no longer required shall be securely disposed of or destroyed

- Disposal methods shall prevent unauthorized recovery or reconstruction of data

8. Roles and Responsibilities

IT / Information Security:

- Implement and maintain data protection controls

- Support secure storage, transmission, and disposal of data

- Monitor compliance with data protection requirements

- Maintain audit evidence

Management / Data Owners:

- Identify and classify data under their responsibility

- Approve access and data sharing where required

- Ensure data protection requirements are met

Users:

- Handle organizational data responsibly and in accordance with this policy

- Protect data from unauthorized access or disclosure

- Report suspected data breaches or data loss incidents promptly

9. Audit and Evidence

Audit evidence shall include data classification records, access control evidence, data sharing approvals, and secure disposal records.

10. Compliance

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

11. Review

This policy shall be reviewed annually or upon significant changes to business operations, regulatory requirements, or data protection risks.