Popular Vehicles & Services

Policy Related to Information Technology Security

BACKUP & RECOVERY POLICY

Document Title : Backup & Recovery 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 backup and recovery of information systems and data to ensure the availability, integrity, and resilience of organizational information assets. This policy supports business continuity, minimizes the impact of system failures or data loss, and meets Information Security and Information Systems audit requirements.

---

2. Scope

This policy applies to all business-critical and sensitive information systems, applications and databases supporting business operations, servers, storage systems, and infrastructure components, including on-premises, cloud-hosted, and hybrid environments.

---

3. Backup & Recovery Principles

The organization shall:

- Ensure regular and reliable backups of critical systems and data
- Protect backup data against unauthorized access, alteration, loss, or corruption
- Maintain the capability to restore systems and data within acceptable timeframes
- Periodically review and improve backup and recovery arrangements

4. Backup Requirements

- Backups shall be performed at defined intervals based on system and data criticality
- Backup scope shall include system configuration, application data, databases, and critical files
- Backup data shall be stored securely, including offsite or cloud-based locations where applicable

- Access to backup data shall be restricted to authorized personnel only

---

5. Recovery Requirements

Recovery procedures shall be in place to restore systems and data following system failure, data corruption, cybersecurity incidents, or operational disruptions

Recovery activities shall prioritize critical business systems to minimize impact

Recovery actions shall be performed by authorized personnel in a controlled manner

---

6. Backup Retention

Backup data shall be retained for a defined retention period based on business, legal, and audit requirements.

Retention periods shall be reviewed periodically.

Backup data beyond retention shall be securely disposed.

---

7. Roles and Responsibilities

IT / Information Security:

Implement and manage backup and recovery controls.

Monitor backup operations and address failures.

Protect backup data and recovery systems.

Maintain audit evidence.

Management / System Owners:

Identify systems and data requiring backup.

Define recovery priorities.

Support recovery decisions.

---

8. Audit and Evidence

Audit evidence shall include backup configurations, backup reports, secure storage evidence, and records of recovery activities.

---

9. Compliance

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

---

10. Review

This policy shall be reviewed annually or upon significant changes to systems, infrastructure, or business requirements.

11.Approval

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

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