BACKUP & RECOVERY POLICY

of

Cosmix LLP

DOCUMENT INFORMATION

Document:	BACKUP & RECOVERY POLICY
Document Number:	COS/POL/05
Version:	1.0
Document Date:	17-06-2026
Prepared By:	HOD-IT
Reviewed By:	CISO
Approved By:	CEO
Classification Level:	Internal

Modification History

Sl. No.	Description of Change	Review Date	Version No.
1	Initial Basic Release	**17-06-2026**	1.0

Contents

1. PURPOSE

- This Policy establishes the framework for backup and recovery of organizational information to ensure availability, integrity and protection of critical business data against accidental deletion, corruption, unauthorized modification, security incidents, or other data loss events.
- The Policy aims to ensure timely data restoration and implementation of appropriate controls to support business continuity.

2. SCOPE

This Policy applies to all information assets and technology resources used, managed, or controlled by LLP, including but not limited to:

- Business documents and records;
- Client-related information;
- Financial and accounting data;
- Applications and databases;
- Cloud-based platforms and storage systems;
- Servers, endpoints, laptops, and other computing devices;
- Backup systems, storage media and recovery solutions.

This Policy applies to all partners, employees, consultants, contractors, interns and third-party service providers who create, access, process, store, or manage organizational information.

3. POLICY REQUIREMENTS - Backup and Recovery Management

A. **Backup requirements** shall be defined based on business criticality, information classification, operational needs and recovery requirements.

B. **Backup and recovery procedures** shall be established considering applicable legal, regulatory, contractual, and business requirements.

C. **Backup frequency and retention periods** shall be determined based on data criticality and business continuity needs.

D. Critical business data shall be **backed up** through approved mechanisms, with secure backup copies maintained where required as part of **Business Continuity & Disaster Recovery process**.

E. **Backup data and storage locations** shall be protected against unauthorized access, loss, damage, or security threats.

F. **Backup activities** and logs shall be **monitored** periodically to identify failures and ensure successful completion.

G. **Restoration testing** shall be conducted periodically to validate backup availability and recovery effectiveness.

H. **Backup media and repositories** shall be securely managed, retained, and disposed of as per applicable retention requirements.

I. **Access to backup systems** shall be restricted to authorized personnel and protected through appropriate security controls.

J. **Cloud service providers and third parties** managing organizational data shall maintain suitable backup and recovery arrangements as per contractual and security requirements.

4. POLICY REVIEW

This Policy shall be reviewed periodically or whenever significant changes occur, including:

i. Changes in technology infrastructure;
ii. Introduction of new applications or systems;
iii. Changes in business operations;
iv. Regulatory or contractual updates;
v. Security incidents or audit observations.

Updates to this Policy shall be reviewed, approved and communicated.

5. EXCEPTION MANAGEMENT

Any exception or deviation from the requirements of this Policy shall:

- Be documented with appropriate justification;
- Be assessed for associated risks;
- Obtain approval from authorized personnel;
- Be periodically reviewed to ensure continued validity.