Backup Encryption Standards Document

1. Purpose

This document defines the standards and requirements for the encryption of backups to ensure the confidentiality, integrity, and availability of organizational data.

2. Scope

These standards apply to all backup systems, storage media, and data retention processes managed by the organization, including on-premises and cloud environments.

3. Encryption Requirements

- All backup data must be encrypted both in transit and at rest.
- Encryption must use approved algorithms and key sizes as specified below.
- Access to encryption keys must be limited to authorized personnel only.

4. Approved Encryption Algorithms

Data State	Algorithm	Key Length
At Rest	AES	256-bit
In Transit	TLS	1.2 or higher

5. Key Management

1. Encryption keys must be stored in a secure, access-controlled environment.
2. Keys must not be stored with the backup data.
3. Regular key rotation is required at least annually, or after any suspected compromise.
4. Retired keys must be securely destroyed.

6. Roles and Responsibilities

- IT Security Team: Defines and reviews backup encryption standards.
- System Administrators: Implements encryption on all backup platforms and ensures compliance.
- Auditors: Validate adherence to standards during regular audits.

7. Compliance and Exceptions

All departments must comply with these standards. Exceptions must be documented and approved by the IT Security Team.

8. Revision History

Date	Version	Description
YYYY-MM-DD	1.0	Initial Draft