Encrypted Data Backup Policy for Financial Institutions

Document Number: [Policy-001]
Effective Date: [YYYY-MM-DD]
Last Reviewed: [YYYY-MM-DD]

1. Purpose

This policy defines the procedures and requirements for encrypting data backups within [Financial Institution Name] to protect sensitive information from unauthorized access, ensuring compliance with regulatory and business standards.

2. Scope

This policy applies to all employees, contractors, and third parties who create, manage, or access backup data for [Financial Institution Name]'s systems, including on-premises and cloud environments.

3. Policy Statement

1. All backups containing sensitive, confidential, or regulated data must be encrypted using strong, industry-standard encryption algorithms.
2. Encryption keys must be securely managed and stored separately from the backup data.
3. Data backups must be protected during creation, storage, transmission, and restoration.
4. Regular testing must be conducted to ensure backup data is recoverable, and encryption does not impede restoration.

4. Roles and Responsibilities

Role	Responsibility
IT Department	Implement and monitor encryption of all backup data, and manage key storage.
Data Owners	Identify and classify data requiring backup and encryption measures.
Compliance Officer	Ensure adherence to applicable legal and regulatory requirements.

5. Backup Encryption Procedures

1. Use AES-256 or stronger encryption standards for all backups.
2. Generate, rotate, and revoke encryption keys according to the institution’s key management policy.
3. Encrypt backups before transferring to off-site or cloud storage.

6. Testing and Verification

- Test restoration of encrypted backups at least quarterly.
- Document results of backup and recovery drills and address any issues immediately.

7. Retention and Disposal

- Maintain encrypted backup files according to the [Institution’s] data retention schedule.

- Securely destroy backups and encryption keys when they are no longer required.

8. Policy Compliance

- Non-compliance may result in disciplinary action and reporting to regulatory authorities.
- Exceptions to this policy must be approved by the Information Security Committee.

9. Review and Updates

This policy will be reviewed annually or as required due to regulatory or technological changes.

Approval:

_____

[Name, Title, Date]