Backup Policy Template

Document Control Information

- **Document Title:** Backup Policy
- **Document Version:** 1.0
- **Last Updated:** [DATE]
- **Document Owner:** [ROLE/NAME]
- **Approved By:** [ROLE/NAME]
- **Next Review Date:** [DATE]

1. Introduction

1.1 Purpose

This Backup Policy establishes [ORGANIZATION NAME]'s requirements for the backup and restoration of information systems and data in accordance with ISO 27001:2022 requirements. It provides a framework for ensuring that critical information is regularly backed up, securely stored, and can be effectively restored when needed.

1.2 Scope

This policy applies to: - All information systems and data owned, operated, or managed by [ORGANIZATION NAME] - All backup and restoration activities performed by or on behalf of the organization - All employees, contractors, and third parties responsible for backup and restoration activities - All environments, including production, development, test, and disaster recovery

1.3 Policy Statement

[ORGANIZATION NAME] is committed to: - Implementing regular and reliable backup procedures for all critical systems and data - Securing backup media and protecting it from unauthorized access, modification, or destruction - Testing backup restoration procedures to ensure data recoverability - Aligning backup strategies with business continuity and disaster recovery requirements - Complying with relevant legal, regulatory, and contractual requirements for data retention

2. Backup Requirements

2.1 Data Classification and Prioritization

- Information assets shall be classified according to their criticality and backup requirements
- Backup frequency and retention shall be based on:
    - Business criticality of the data
    - Rate of data change
    - Recovery point objective (RPO)
    - Legal, regulatory, and contractual requirements
    - Operational requirements
- A backup inventory shall be maintained, documenting backup requirements for each system

2.2 Backup Frequency and Scheduling

- Critical systems and data shall be backed up according to the following minimum schedule:
    - [SPECIFY BACKUP SCHEDULE FOR DIFFERENT CATEGORIES]
    - Example:
        - Critical production databases: Full backup daily, transaction logs every hour
        - Business applications: Full backup daily
        - User data: Full backup weekly, incremental backup daily
        - System configurations: After any change
- Backup schedules shall be designed to minimize impact on system performance and availability
- Backup windows shall be clearly defined and communicated

2.3 Backup Types

The following backup types shall be used as appropriate: - Full backup: Complete backup of all selected files and folders - Incremental backup: Backup of data changed since the last backup of any type - Differential backup: Backup of data changed since the last full backup - Transaction log backup: Backup of database transaction logs - System state backup: Backup of critical operating system components - Image backup: Complete system or disk image

2.4 Backup Retention

- Backup retention periods shall be defined based on:
    - Business requirements

    - Legal and regulatory requirements
    - Contractual obligations
    - Storage capacity constraints
- Minimum retention periods shall be:
    - [SPECIFY RETENTION PERIODS FOR DIFFERENT CATEGORIES]
    - Example:
        - Daily backups: [30] days
        - Weekly backups: [3] months
        - Monthly backups: [12] months
        - Annual backups: [7] years
- Backup media shall be securely destroyed at the end of its retention period

3. Backup Storage and Protection

3.1 Backup Storage Locations

- Backups shall be stored in multiple locations to protect against site-specific threats
- At least one copy of critical backups shall be stored offsite
- Physical separation between primary systems and backup storage shall be maintained
- Cloud-based backup storage shall comply with data sovereignty requirements

3.2 Backup Media Security

- Backup media shall be protected against unauthorized access, modification, or destruction
- Physical backup media shall be stored in secure, environmentally controlled facilities
- Backup media shall be clearly labeled without revealing sensitive content
- Media handling procedures shall be documented and followed
- Media shall be verified before reuse or disposal

3.3 Backup Encryption

- Backups containing sensitive or confidential information shall be encrypted
- Encryption keys shall be managed according to the Cryptography Policy
- Encryption keys shall be backed up separately from the encrypted data
- Encryption shall be applied before data leaves the secure environment

3.4 Access Control

- Access to backup systems and media shall be restricted to authorized personnel
- Access rights shall be regularly reviewed and updated
- Authentication and authorization controls shall be implemented
- Access to backup systems and media shall be logged and monitored

4. Backup Verification and Testing

4.1 Backup Verification

- Backup completion shall be automatically verified
- Backup logs shall be reviewed [DAILY/WEEKLY] for errors or warnings
- Backup integrity shall be verified through automated checks
- Failed backups shall be investigated and remediated promptly

4.2 Restoration Testing

- Restoration procedures shall be documented for all critical systems
- Restoration tests shall be performed according to the following schedule:
  - Critical systems: Quarterly
  - Important systems: Semi-annually
  - Other systems: Annually
- Restoration tests shall include verification of data integrity and completeness
- Restoration tests shall be documented, including any issues encountered
- Restoration tests shall be performed in isolated environments to avoid production impact

4.3 Recovery Time Objectives

- Recovery Time Objectives (RTOs) shall be defined for all systems
- Restoration procedures shall be designed to meet defined RTOs
- Actual restoration times shall be measured during testing
- Deviations from RTOs shall be addressed through process improvements

5. Backup Operations

5.1 Backup Documentation

The following documentation shall be maintained: - Backup procedures for all systems - Restoration procedures for all systems - Backup schedules and retention periods - Backup system configurations - Backup inventory and media tracking - Backup verification and test results

5.2 Backup Monitoring and Reporting

- Backup systems shall be monitored for successful completion
- Automated alerts shall be configured for backup failures
- Backup status reports shall be generated [DAILY/WEEKLY]
- Backup capacity and performance shall be monitored
- Backup trends shall be analyzed to identify potential issues

5.3 Backup System Security

- Backup systems shall be included in security assessments
- Backup systems shall be patched and updated regularly
- Backup system access shall be restricted and monitored
- Backup network traffic shall be secured
- Backup systems shall be protected from malware

5.4 Backup Media Management

- Media shall be tracked throughout its lifecycle
- Media shall be stored according to manufacturer specifications
- Media shall be tested regularly for reliability
- Media shall be replaced according to manufacturer recommendations
- Media shall be securely destroyed at end-of-life

6. Roles and Responsibilities

6.1 IT Department

- Implement and maintain backup systems
- Execute backup procedures according to schedule
- Monitor backup completion and address failures
- Perform restoration tests
- Maintain backup documentation

6.2 System Owners

- Define backup requirements for their systems
- Approve backup schedules and retention periods
- Participate in restoration testing
- Verify restored data integrity and completeness

6.3 Information Security Team

- Review backup security controls
- Ensure compliance with this policy
- Provide guidance on backup encryption
- Include backup systems in security assessments

6.4 Compliance Team

- Ensure backup retention meets legal and regulatory requirements
- Review backup procedures for compliance
- Participate in backup audits
- Provide guidance on data retention requirements

7. Compliance and Exceptions

7.1 Compliance Monitoring

- Regular audits shall verify compliance with this policy
- Backup logs and reports shall be reviewed for compliance
- Restoration tests shall verify recoverability
- Non-compliance shall be reported and addressed

7.2 Exceptions

Exceptions to this policy shall be: - Documented with justification - Risk-assessed and approved by the Information Security Manager - Time-limited and regularly reviewed - Accompanied by compensating controls where appropriate

8. Related Documents

- Information Security Policy
- Data Protection Policy
- Business Continuity Plan
- Disaster Recovery Plan
- Data Retention Policy
- Cryptography Policy
- [LIST OTHER RELEVANT POLICIES AND PROCEDURES]

9. Approval

This Backup Policy is approved by:

Name: ________________________ Position: ______________________ Date: _________________________ Signature: _____________________