# Backup Management Policy

## Document Control

* **Version:** 1.0
* **Last Updated:** 2024-12-18
* **Classification:** Internal
* **Owner:** Information Security Team
* **Next Review Date:** 2025-12-18

## Executive Summary

This document outlines the comprehensive requirements for backup management policy. The policy is designed to ensure consistent and secure practices across the organization.

## Purpose and Objectives

This policy defines requirements for backup management policy with the following objectives: 1. Establish clear governance and accountability 2. Ensure regulatory compliance 3. Protect organizational assets and data 4. Enable secure business operations

## Scope

This policy applies to: - All employees and contractors - All systems and data - Third-party service providers - Business partners with access to systems

## Definitions and Terminology

| **Term** | **Definition** |
| --- | --- |
| Control | A measure designed to provide reasonable assurance regarding the achievement of objectives |
| Policy | A formal statement of rules and requirements that must be met |
| Standard | A mandatory requirement that supports policies |
| Procedure | A documented method to implement policies and standards |

## Policy Requirements

### BM-01 - Backup Configuration

#### Control Information

| **Type** | **Theme** |
| --- | --- |
| Corrective | Process |

#### Policy Description

Organization configures redundant systems or performs periodic backups of data to resume system operations in the event of a system failure.

#### Implementation Requirements

1. Ensure that Backup and Restoration process is established, documented and communicated to all the relevant stakeholders.
2. Ensure that all the information systems have redundancy or should be backed up periodically. Periodicity of the backup should be defined basis the criticality of the information system and data.
3. Check the backup configuration for all the storage/database resources whether on-prem or on cloud.
4. Ensure that alert are in place for backup failures and all backup failures are handled appropriately.

#### Testing Procedures

1. Inspect documentation to determine whether requirements for the configuration of redundant systems or performance of periodic backups of data to resume system operations are defined.
2. Inspect redundancy or system backup configurations for production systems to determine type, frequency, and storage of backups.
3. Inspect sample alerts for failed backups and validate the remediation steps.

#### Audit Requirements

Evidence Required:

| **ID** | **Domain** | **Title** |
| --- | --- | --- |
| E-BM-01 | Backup Management | Backup Management Policy |
| E-BM-07 | Backup Management | Backup Configuration Evidence |

### BM-02 - Resilience Testing

#### Control Information

| **Type** | **Theme** |
| --- | --- |
| Detective | Process |

#### Policy Description

Organization performs annual backup restoration or data replication tests to confirm the reliability and integrity of system backups or recovery operations.

#### Implementation Requirements

1. Ensure that the requirement for backup restoration testing is defined and documented appropriately.
2. Ensure that backup restoration testing is performed on an annual basis and ensure that the integrity of backup restores are maintained.

#### Testing Procedures

1. Inspect relevant documentation to determine whether requirements for annual backup restoration or failover and failback tests have been defined.
2. Inspect annual backup restoration, or failover and failback tests to determine whether Organization has tested the reliability and integrity of system backups.

#### Audit Requirements

Evidence Required:

| **ID** | **Domain** | **Title** |
| --- | --- | --- |
| E-BM-01 | Backup Management | Backup Management Policy |
| E-BM-02 | Backup Management | Backup Restoration Test Results |

## Framework References

| **Control ID** | **Framework** | **Reference** |
| --- | --- | --- |
| BM-01 | NIST CSF | PR.IP-4 |
| BM-02 | NIST CSF | PR.IP-4 |

## Framework Reference Mapping

| **Framework** | **Reference** | **Controls** |
| --- | --- | --- |
| NIST CSF | PR.IP-4 | BM-01, BM-02 |

## Compliance and Monitoring

### Compliance Measurement

* Regular assessments will be conducted to ensure compliance
* Automated monitoring tools will be used where applicable
* Quarterly compliance reports will be generated

### Non-Compliance

Violations of this policy may result in: 1. Disciplinary action 2. Termination of employment 3. Legal action if warranted

## Review and Updates

* This policy will be reviewed annually
* Updates will be made in response to:
  + Changes in business requirements
  + New security threats
  + Regulatory changes
  + Lessons learned from incidents

## Document History

| **Version** | **Date** | **Changes** | **Approved By** |
| --- | --- | --- | --- |
| 1.0 | 2024-12-18 | Initial Release | Information Security Team |