**Cybersecurity Templates**

**Backup and Restoration Plan (BRP)**

**August 2025**

|  |  |  |
| --- | --- | --- |
| **Logo** | **< Company Name>** | **Normal** |

|  |
| --- |
| **Backup and Restoration Plan (BRP)** |

|  |  |  |  |
| --- | --- | --- | --- |
| **Version:** |  | **Approved By:** |  |
| **Last Review Date:** |  | **Next Review Date:** |  |

Contents

[Backup and Restoration Plan (BRP) 4](#_Toc206710426)

[1. Authority and Review 4](#_Toc206710427)

[1.2 Version Control 4](#_Toc206710428)

[2. Purpose and Objectives 4](#_Toc206710429)

[2.1 Purpose 4](#_Toc206710430)

[2.2 Objectives 4](#_Toc206710431)

[3. Standards and Frameworks 4](#_Toc206710432)

[4. Scope and Applicability 5](#_Toc206710433)

[5. Roles and Responsibilities 5](#_Toc206710434)

[5.1 Governance Roles 5](#_Toc206710435)

[5.2 Contact Information 5](#_Toc206710436)

[6. Backup Strategy and Requirements 5](#_Toc206710437)

[6.1 Backup Methods 5](#_Toc206710438)

[6.2 Frequency and Retention 6](#_Toc206710439)

[6.3 Storage Locations 6](#_Toc206710440)

[6.4 Encryption & Key Management 6](#_Toc206710441)

[7. Data Restoration Process 6](#_Toc206710442)

[7.1 Restore Request Workflow 6](#_Toc206710443)

[7.2 Validation 6](#_Toc206710444)

[7.3 Escalation 7](#_Toc206710445)

[8. Communications and Escalation 7](#_Toc206710446)

[9. Testing and Validation 7](#_Toc206710447)

[10. Continuous Improvement 7](#_Toc206710448)

[Appendices 7](#_Toc206710449)

# Backup and Restoration Plan (BRP)

# 1. Authority and Review

**1**.1 Document Control and Review

|  |  |  |  |
| --- | --- | --- | --- |
| **Author** |  | **Owner** |  |
| **Date Created** |  | **Last Reviewed By** |  |
| **Last Review Date** |  | **Next Review Due Date** |  |

## 1.2 Version Control

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date of Approval** | **Approved By** | **Description of Change** |
|  |  |  |  |

# 2. Purpose and Objectives

## 2.1 Purpose

The purpose of this Backup and Restoration Plan (BRP) is to ensure that critical organizational systems, applications, and data are reliably backed up, protected, and recoverable in the event of an incident, disaster, or system failure.

## 2.2 Objectives

* Protect organizational information assets from loss or corruption.
* Ensure backups meet Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO).
* Provide clear restoration processes to minimize downtime.
* Support compliance with ISO/IEC 27031, NIST SP 800-34, and other relevant standards.
* Promote business continuity and operational resilience.

# 3. Standards and Frameworks

This BRP is designed in alignment with:

* **ISO/IEC 27031:2011** – ICT readiness for business continuity.
* **NIST SP 800-34 Rev.1** – Contingency Planning Guide for Federal Information Systems.
* **NIST SP 800-184** – Guide for Cybersecurity Event Recovery.
* **CIS Controls v8** – Data Recovery Practices.
* **FFIEC Business Continuity Management Handbook**.

# 4. Scope and Applicability

This plan applies to:

* All enterprise IT systems, applications, databases, storage platforms, and network devices.
* All data classified as **Critical** or **Confidential** per the organization’s Data Classification Policy.
* On-premises, cloud, and hybrid environments.
* All employees, contractors, and third parties handling backups or restoration activities.

# 5. Roles and Responsibilities

## 5.1 Governance Roles

* **Executive Sponsor** – Provides strategic oversight, approves plan updates.
* **Backup and Restoration Plan (BRP) Owner** – Maintains the plan, coordinates reviews/tests.
* **IT Backup Team** – Executes daily/weekly/monthly backups, verifies integrity.
* **Application/Data Owners** – Validate that restored systems meet operational needs.
* **Information Security Officer** – Ensures compliance, audits, and risk assessments.
* **End Users** – Report issues and request data restoration when needed.

## 5.2 Contact Information

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Title** | **Role** | **Contact Details** |
|  |  |  |  |

# 6. Backup Strategy and Requirements

## 6.1 Backup Methods

* **Full Backup** – All data, performed weekly.
* **Incremental Backup** – Changes since last backup, performed daily.
* **Differential Backup** – Changes since last full backup.
* **Mirror Backup** – Exact real-time replication.

## 6.2 Frequency and Retention

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Data Type** | **Frequency** | **Retention Period** | **Location** | **Method** |
| Critical Systems | Daily (incremental) + Weekly (full) | 12 months | Offsite + Cloud | Encrypted |
| Databases | Every 6 hours | 6 months | Onsite + Offsite | Encrypted |
| Virtual Machines | Weekly | 6 months | Offsite/Cloud | Image backup |

## 6.3 Storage Locations

* **Primary Site:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* **Offsite Facility:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* **Cloud Service Provider:** \_\_\_\_\_\_\_\_\_\_\_

## 6.4 Encryption & Key Management

* All backups must be encrypted in transit and at rest.
* Keys stored in a secure Key Management System (KMS).
* Key rotation should occur every 12 months or after a compromise.

# 7. Data Restoration Process

## 7.1 Restore Request Workflow

1. User submits a restore request.
2. IT Backup Team validates request.
3. Approval from BRP Owner (if sensitive data).
4. Restore initiated in the staging environment.
5. Data/application validated.
6. Full production restoration executed.

## 7.2 Validation

* Integrity checks (hash verification).
* Functional testing (application/system works as expected).
* Documentation of evidence in the restore log.

## 7.3 Escalation

If restoration exceeds RTO, escalate to:

* Executive Sponsor
* Business Continuity/DR Team

# 8. Communications and Escalation

* **Internal Communications:** Updates shared with IT, security, and business stakeholders.
* **External Communications:** Engage vendors, regulators, or cloud providers as required.
* **Escalation Matrix:** Defined thresholds (e.g., failure of two consecutive restore attempts).

# 9. Testing and Validation

* **Quarterly Restore Tests** – Validate ability to restore critical systems.
* **Annual Full Recovery Exercise** – Simulated disaster recovery drill.
* **Documentation** – Keep logs, test results, and corrective actions.
* **Lessons Learned** – Feed outcomes into plan improvements.

# 10. Continuous Improvement

* The BRP must be reviewed **annually** or after any significant incident/test.
* Updates logged in the **Change Log**.
* Lessons learned integrated into updated procedures.

# Appendices

**Appendix A – Contact List**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Department** | **Role** | **Phone** | **Email** |
|  |  |  |  |  |

**Appendix B – Backup Job Catalog**

* List of scheduled jobs
* Systems
* Backup types

**Appendix C – Restoration Request Form**  
Standardized form for requesting restores.

**Appendix D – Validation Checklist**  
Step-by-step validation of restored data.

**Appendix E – Change Log**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Description of Change** | **Author** |
|  |  |  |  |