DATA BACKUP & RECOVERY POLICY

*Revision: r1.0*

*Effective Date:*

*Classification: INTERNAL*

**Internal INFORMATION**

This is a proprietary document and is the property of XXXX it contains information that is proprietary, or otherwise restricted from disclosure. If you are not an authorised recipient, please return this document to the above-named owner(s). Dissemination, distribution, copying or use of this document in whole or in part by anyone other than the intended recipient is strictly prohibited without prior written permission of XXXX

Table of Contents

1. Introduction 3

1.1 Document Definition 3

1.2 Objective 3

1.3 Scope 3

1.3.1 Applicability to employee 3

1.3.2 Applicability to External Parties 3

1.3.3 Applicability to Assets 3

1.4 Related Documents / References 3

2. Policy Statements 4

2.1 Backup Frequency 4

2.2 Backup and Recovery Statements 4

3. Policy Compliance & Enforcement 5

3.1 Compliance Measures 5

3.2 Enforcement 5

4. Exception Process / Glossary 6

4.1 Exception Process 6

4.2 Glossary / Acronyms 6

5. Document Management 7

5.1 Document Revision Log 7

5.2 Document Ownership 7

5.3 Document Coordinator 7

5.4 Document Approvers 7

5.5 Document Distribution 7

# 

# Introduction

## Document Definition

This document is a Policy.

For a full description of document types, see *XXXX-POL-ALL-001 - Information Security Policy Framework*.

## Objective

The primary objectives of data backup and recovery is to maintain the integrity of data, minimizing the effects of errors on end users and restoring services as quickly as possible.

## Scope

### Applicability to employee

XXXX refers to XXXX as well as its majority-owned subsidiaries and joint ventures (if applicable). This Policy applies to all employees, officers, members of Board of Directors, and all consultants, and contractors.

### Applicability to External Parties

Relevant Policy statements will apply to any external party and be included in contractual obligations on a case-by-case basis.

### Applicability to Assets

This Policy applies to all information assets globally owned by XXXX, or where XXXX has custodial responsibilities.

## Related Documents / References

* *XXXX-POL-ALL-001 - Information Security Policy Framework*
* *XXXX-POL-ALL-004 - Data Classification Policy*
* *XXXX-POL-ALL-005 - Data Handling & Retention Policy*
* *XXXX-STD-ALL-011 - Data Handling, Destruction & Retention Standard*

# Policy Statements

## Backup Frequency

Backup and recovery of data from critical business applications shall be performed on a regular basis as determined by the system owner or delegate.

## Backup and Recovery Statements

* If required data shall be backed up to tape or disk and taken to an offsite location daily
* Information system owners shall ensure that adequate backup and system recovery procedures are in place for all critical data
* Backup of critical business data shall be restored and validated by IT and Information Security Officer at least bi-annually
* IT Management shall ensure that safeguards are in place to protect the integrity of the data files during the recovery and restoration of data files, especially where such files may replace more recent files
* Data on backup tapes / disk shall be duly protected to ensure data integrity when backup tapes or disk are being taken to an offsite location.
* Critical but non-database documents must be backed up unto the fileserver by document owners. Departmental Heads must ensure compliance to safeguard critical documents from residing on personal laptops and computers.
* Restore of backed up data should be carried out yearly in a test and controlled environment
* Data back-ups shall be stored at a location that is enough distance from point of data origin to avert any damage from a disaster affecting the latter. Secure enclosures shall be used to store data backup media and shall be given an appropriate level of physical and environmental protection consistent with XXXX’s policies for protecting such areas.
* Where the confidentiality of data is paramount, back-ups shall be protected by means of encryption.
* Full data and system backups of all XXXX’s applications shall be undertaken at least annually. Additional backup frequency shall be determined based on specific system requirements. Full system backups shall however be taken prior to any hardware changes, modification of the applications or operating systems or software.
* Data recovery tests shall be carried out at least annually. Results of the test would be documented and used for improvements of subsequent tests

# Compliance & Enforcement

## Compliance Measures

If applicable, compliance with the above Policy can be measured by the following criteria. Example evidence will vary depending on any supporting guidelines implemented to support this Policy. The following list is not exhaustive, and all example evidence types may not be required to validate compliance.

Evidence of compliance can be presented in hard copy or electronic format.

|  |  |
| --- | --- |
| **Criteria** | **Example Evidence** |
| Review critical business applications | * Check report of data backup test conducted |
| Identify information data owners have classified as critical | * Ensure critical data are been backed up correctly |
| Protection of backed up files and tapes | * Check that logical and physical protection of backed up files and tapes are adequate |
| Critical data specified to be protected by encryption | * Confirm that data that have been specified to be protected by encryption are protected by secure encryption technology |

## Enforcement

All staff of XXXX must comply with all Information Security Policies. Failure to comply with these policies may result in disciplinary action in accordance with the current XXXX Human Resources policy. Disciplinary actions may include, but are not limited to:

* verbal and/or written warnings;
* instant dismissal; and
* actions by judicial and regulatory authorities.

# Exception Process / Glossary

## Exception Process

Non-compliance with the Policy statements described in this document must be reviewed and approved in accordance with the Exception Process defined in XXXX-POL-ALL-001 *- Information Security Policy Framework*.

## Glossary / Acronyms

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

# 

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
|  |  |  |  |
|  |  |  |  |

## Document Ownership

This Policy is owned by the YYYY.

## Document Coordinator

This Policy is coordinated by the YYYY.

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
|  |  |  |
|  |  |  |

## Document Distribution

The Document Owner controls distribution of this document. The distribution is as follows:

* All Staff