DISASTER RECOVERY POLICY

*Revision: r1.0*

*Effective Date: ddmmyyyy*

*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 Employees 3

1.3.1 Applicability to External Parties 3

1.3.2 Applicability to Assets 3

1.4 Related Documents / References 3

2. Policy Statements 4

2.1 Planning Process 4

2.2 Plan Development 4

2.3 Plan Specifications 4

2.4 Plan Contingencies 4

2.5 Documentation 5

2.6 Plan Review, Testing and Maintenance 5

3. Policy Compliance & Enforcement 6

3.1 Compliance Measures 6

3.2 Enforcement 6

4. Exception Process / Glossary 7

4.1 Exception Process 7

4.2 Glossary / Acronyms 7

5. Document Management 8

5.1 Document Revision Log 8

5.2 Document Ownership 8

5.3 Document Coordinator 8

5.4 Document Approvers 8

5.5 Document Distribution 8

# 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 objective of this policy is to provide information security requirements for the development and maintenance of Disaster Recovery Plans to enable XXXX (XXXX) to withstand the prolonged unavailability of critical information and systems and the recovery of IT services in the event of a disaster.

Disaster Recovery (DR) is best described as the plans and activities designed to recover technical infrastructure and restore critical business applications to an acceptable condition. DR is a component of Business Continuity Management, which is the process of ensuring that essential business functions continue to operate during and after a disaster. The overall requirements for Business Continuity are addressed in *XXXX-POL-ALL-008- Business Continuity Management Policy*.

## Scope

### Applicability to Employees

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-008- Business Continuity Management Policy*
* *XXXX-POL-ALL-012- Incident Response Policy*
* *XXXX-PRC-ALL-006 Incident Response Procedure(s)*
* *XXXX-PRC-ALL-008 – Business Continuity Plan*

# Policy Statements

## Planning Process

A formal process for developing disaster recovery plans must be established and aligned with the Business Continuity Planning requirements set forth in *XXXX-POL-ALL-008 - Business Continuity Management Policy*.

## Plan Development

The procedures for developing disaster recovery plans must specify that plans be:

* provided for all critical IT components of the business;
* based on the results of a documented Risk Assessment (RA) and/or Business Impact Analysis (BIA);
* distributed to all individuals who would require them in case of an emergency, and;
* kept up to date and subject to standard / local change management procedures.

## Plan Specifications

Disaster recovery plans must contain:

* conditions for their invocation;
* critical timescales associated with the supported business services / processes;
* a priority list of services to be recovered;
* a schedule of key tasks that include responsibilities for each task;
* procedures to be followed for completing key tasks (e.g., emergency recovery, post recovery, fail back, and resumption);
* sufficient detail so they may be carried out by individuals who do not normally carry out these responsibilities, and;
* a requirement that relevant staff be informed of their disaster recovery responsibilities and trained to discharge them.

## Plan Contingencies

Contingency arrangements must be made in the event of prolonged unavailability of:

* key individuals;
* systems or applications;
* business information (in paper or electronic form);
* physical access to IT areas or facilities;
* essential services to IT areas or facilities (e.g., electricity, gas, water);
* communication lines, and;
* relevant documentation.

## Documentation

Disaster Recovery Plans must be documented, safeguarded, and made available to all appropriate parties. Copies of disaster recovery plans must also be stored at easily accessible off-site locations.

## Plan Review, Testing and Maintenance

Disaster recovery plans must be reviewed by the Security Committee at least annually and when significant application or infrastructure changes are made. Plans must be tested periodically and at least once per year, and include realistic simulations involving the business users and IT staff. The results of DR tests must be documented, reviewed, and approved by appropriate management.

# Policy 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** |
| For a selection of plan development procedures, evidence that all required components are included | * Plan development procedures document * Interviews with key plan development personnel |
| For a selection of critical IT systems and/or applications, evidence that a Business Impact Analysis (BIA) was performed | * BIA output form * BIA report |
| For a selection of Disaster Recovery Plans, evidence that plan contingencies have been developed | * Plan document |
| For a selection of Disaster Recovery Plans, evidence that the plans were reviewed annually, at a minimum | * Physical sign-off on plan document * Email or other electronic workflow tool approval |
| For a selection of Disaster Recovery Plan documentation, evidence that the plans are communicated to appropriate personnel and maintained in a secure repository | * Interviews with personnel (currently occupying the associated role) named in the plan * DR test report and/or notes * File permissions on network drives containing plans |
| For a selection of Disaster Recovery Plans, evidence that all required specifications are included | * Plan document * DR test report and/or notes * DR tool output |
| For a selection of Disaster Recovery Plans, evidence that the plan is tested at least once a year and maintained | * DR test report and/or notes * Last modification date on plans * Email or other electronic workflow tool approval |

## 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

|  |  |
| --- | --- |
| BIA | Business Impact Analysis |
| RA | Risk Assessment |

# Document Management

## Document Revision Log

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Editor** | **Revision #** | **Description of Change** |
| July 10, 2020 | Michael Oyerinde | r1.0 | Approval of new policy |
| February 9, 2021 | Michael Oyerinde | r1.1 | Approval by Executive Committee |

## Document Ownership

This Policy is owned by the Executive Committee.

## Document Coordinator

This Policy is coordinated by the COO.

## Document Approvers

|  |  |  |
| --- | --- | --- |
| **Approver Name** | **Signature** | **Date** |
| Executive Committee |  | February 9, 2021 |
|  |  |  |

## Document Distribution

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

* All Staff