BUSINESS CONTINUITY MANAGEMENT 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 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 Plan Development and Maintenance 4

2.2 Business Impact Analysis 4

2.3 Recovery Plan Requirements 4

2.4 Operational Resilience & Redundancy 4

2.5 Plan Review 4

2.6 Plan Testing 5

2.7 Documentation 5

2.8 Information Security Continuity 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 enable the XXXX proactively identify and plan to minimise the impact of risks that could affect its objectives, operations and information assets. The business continuity framework will provide for the development of processes, and the availability of information resources that ensure the continued achievement of the XXXX's critical business objectives.

It will provide a robust framework that allows the XXXX to:

* better understand risks;
* realize the potential for different types of disruption that may impact critical business objectives; and,
* to better plan for management of those disruptions and to put in place business improvement now, to reduce the likelihood and/or consequence of significant disruption.

## 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-013 - Disaster Recovery Policy*
* *XXXX-PRC-ALL-008 - Business Continuity and Disaster Recovery Plan*

# Policy Statements

## Plan Development and Maintenance

Business process owner(s) are accountable for developing and maintaining documented Business Continuity Plans for their respective areas.

## Business Impact Analysis

Business Continuity Plans must be developed that cover all essential and critical business activities based on the results of a periodically performed Business Impact Analysis (BIA) conducted on business processes to ensure appropriate business focus and to identify recovery time objectives.

## Recovery Plan Requirements

Business Continuity Plans must be developed with requirements based on the specific risks associated with the process or system. All staff must be made aware of the Business Continuity Plan and their own respective roles.

Plans must include, but are not limited to, the following information:

* Executive Summary
* Key Assumptions
* Identified Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO)
* Long-term vs. Short-term Outage Considerations
* Disaster Declaration / Plan Activation Procedures (e.g., Communication plan, mobilisation plan)
* Key Contacts / Calling Tree(s)
* Roles / Responsibilities (e.g., Recovery Teams)
* Alternate Site / Lodging
* Asset Inventory
* Detailed Recovery Procedures
* Disaster Recovery Plans, where applicable
* Event and recovery status reporting to appropriate stakeholders and impacted employees

## Operational Resilience & Redundancy

Where appropriate, both operational resilience and redundancy measures will be built in to production systems.

## Plan Review

Business Continuity Plans must be reviewed annually (and the plan documentation updated accordingly), or when significant business or technology changes occur. Business Continuity Plans must be formally approved by the appropriate business unit department head.

## Plan Testing

Business Continuity Plans must be tested periodically and at least once a year.

## Documentation

Business Continuity Plans must be well documented, safeguarded, and made available to all appropriate parties. Copies of Business Continuity Plans must also be stored at off-site locations and be made easily accessible in the event they are required.

## Information Security Continuity

Throughout the business continuity recovery stage, information security is factored to every step to ensure the XXXX can still maintain an expected level of information security throughout the recovery process.

# 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 critical business functions, evidence that a Business Continuity Plan exists and contains the relevant information, per 2.4 above.  Event and recovery status reporting to appropriate stakeholders and impacted employees | * Plan document * BC test report and/or notes |
| For a selection of critical business functions, evidence that a Business Impact Analysis (BIA) was performed | * BIA output form * BIA report |
| For a selection of Business Continuity 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 Business Continuity 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 * BC test report and/or notes * File permissions on network drives containing plans |
| For a selection of Business Continuity Plans, evidence that the plan is tested at least once a year and maintained based on the results | * BC 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

|  |  |
| --- | --- |
| Business Continuity (BC) | The process for recovering and/or restoring partially or completely interrupted business process or function within a predetermined time after an unplanned disruption. |
| Business Impact Analysis (BIA) | An assessment used to determine the business units, operations and processes that are essential to the survival of the business. |
| Disaster Recovery (DR) | The plans and activities for recovering technical infrastructure and restoring critical business systems/applications to an acceptable condition. |
| Recovery Point Objectives (RPO) | The acceptable amount of data loss measured in time. |
| Recovery Time Objectives (RTO) | The duration of time and a service level within which a business process must be restored after an unplanned disruption in order to avoid unacceptable consequences associated with a break in business continuity. |

# 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