LOGO

**Policy Document**

**Business Continuity Management Policy**

**Effective Date: (At Approval)**

**Effective Date: (At Approval)**

Archive Number:

Policy Unique Number:

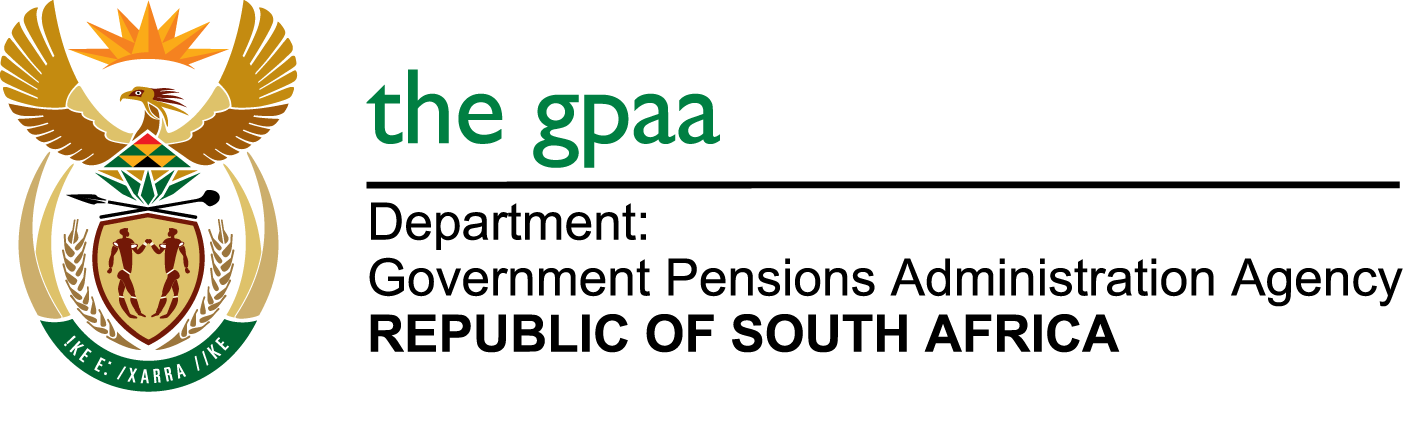
Document Classification:

Confidential

© [Department] 2019

Document Versions

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Revision Date** | **Prepared / Revised by** | **Business Unit** | **Status** |
| V 0.1 |  |  |  |  |
| V 0.2 |  |  |  |  |
| V 0.3 |  |  |  |  |
| V 0.4 |  |  |  |  |
| V 0.5 |  |  |  |  |
| V.0.6 |  |  |  |  |
| V 0.7 |  |  |  |  |
| V 0.8 |  |  |  |  |
| V 0.9 |  |  |  |  |

**Approval / Adoption Document**

Policy Name: **Business Continuity Management Policy**

Archive Number: **??**

Unique Policy Number: **??**

Document Classification: **Confidential**

Prepared by: **Strategy and Policy**

Recommended / Not Recommended / Comments

**POLICY OWNER:**

**??**

**DATE:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Recommended / Not Recommended / Comments

**??**

**GENERAL MANAGER: HUMAN RESOURCES (Acting)**

**DATE**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Recommended / Not Recommended

**??**

**SENIOR MANAGER: COMMUNICATIONS**

**DATE:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Recommended / Not Recommended

**??**

**HEAD: LEGAL SERVICES AND SECRETARIAT**

**DATE:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Recommended / Not Recommended

**??**

**GENERAL MANAGER: STRATEGIC SUPPORT (Acting)**

**DATE:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Recommended / Not Recommended

**??**

**CHAIRPERSON: POLICY STEERING COMMITTEE**

**DATE:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Approved / Not Approved

Effective date:

**??**

**DIRECTOR GENERAL**

**DATE:**

Table of Contents

[1 Background of policy 4](#_Toc524504722)

[2 Policy environment 4](#_Toc524504727)

[3 Policy 4](#_Toc524504728)

[4 Policy informing process and legislative framework 5](#_Toc524504737)

[5 Implementation overview 5](#_Toc524504738)

[6 Limitations and conditions 7](#_Toc524504773)

[7 Roles and responsibilities 8](#_Toc524504774)

[8 Concluding comments 10](#_Toc524504826)

[9 Document Reference Library 10](#_Toc524504828)

[10 Business Areas impacted by this Policy 10](#_Toc524504829)

[11 Regulatory Framework 10](#_Toc524504830)

[12 Descriptions of Abbreviations and Concepts 11](#_Toc524504831)

# Background of policy

## Introduction

### In this dynamic world institutions are subject to disruptions that tend to hamper service delivery. Such disruptions contain high and low risks that impact the institution’s day-to–day operations. These risks also apply to the [Department]) that is mandated to deliver services to the targeted population without any operational disturbance, even when a disaster has occurred.

## 

## Purpose

### This [Department] policy on Business Continuity Management (BCM) attempts to help identify potential threats within the organisation and the impact that those threats might have on business operations, therefore, providing a framework that will build organisational resilience and establish an effective response that preserves the value given by the organisation.

# Policy environment

2.1 The [Department] operates within the landscape of ??? within government administration.

2.2 The [Department]’s operational duties are performed from the Head Office in [City] and from the regional and satellite offices.

# Policy

## Aim

3.1 The aim of this policy is to establish principles and responsibilities for the BCM programme within the [Department]. It seeks to steer a good practice oriented BCM programme in order to increase the institution’s readiness against disasters that may threaten delivery of services. The policy also attempts to drive the institution towards foreseeing and mitigating threats or risks that may hamper critical activities of the business after the commencement of a disaster.

## The objectives of this policy are to:

### identify the main threats in the organisation and possible threats to business processes;

### determine response tactics to losses that the business might incur due to a disaster;

### establish business unit plans that ensure the continuity of business;

### drive all BCM activities to follow good practices in order to attain a full programme lifecycle;

### outline tools to be used throughout the BCM programme lifecycle; and

### outline responsibilities of tactical committees and enhance BCM awareness within the entire the [Department].

# Policy informing process and legislative framework

4.1 Constitution of the Republic of South Africa Act (No. 108 of 1996)

4.2 ISO 22301

4.3 BCM Good Practice guide 2018

4.4 Occupational Health and Safety Act as amended by Occupational Health and Safety Amendment Act (No. 181 of 1993)

4.5 Batho Pele Principles

4.6 King IV codes of Corporate Governance

4.7 The Public Finance Management (Act No. 29 of 1999) as amended

4.8 National Archives and Record Service of South Africa act of 1996

# Implementation overview

## Business Continuity Awareness:

### Training and Development of officials on Business Continuity Management and its operation will be offered as per the Human Resource training policy.

### The employer shall endeavour to make the employees aware of BCM so that they may familiarise themselves with structures of Business Continuity, including emergency BC contact number.

### The organisation shall affiliate with relevant stakeholders of Business Continuity within the Republic of South Africa and within the Public sector.

### BCM shall communicate regularly with employees about Business Continuity, its meaning and Business Continuity scenarios intended for the institution.

### A Business Continuity budget shall reside with the Strategy office.

### A Disaster Recovery budget shall reside with the ICT office

### The BC Risk management Budget shall reside with the Risk Management Office.

## Programme Management:

### BC Sub-committees that are to cascade BC to operational levels shall be established from the BC Committee and other committees that should be established to ensure the effective implementation of BCM within the [Department].

### The committee members shall be nominated by the Accounting Officer through appointment letters signed by both the nominated member and the DG.

### Recognised DBC unions shall be represented in the BC Committee.

### The activities of the established committees shall be regulated though a TOR drafted by the members with the assistance of the relevant experts.

## BCM Strategy:

### A BCM strategy shall be determined for the organisation and relevant stakeholders will be identified for its execution.

### The BCM strategy shall be cascaded down to the operational level, and each business unit must support the strategy by drafting a BC Plan.

### The BC Committee and its different sub-committees and the chief co-ordinator shall ensure synergy between the different structures to coordinate BCM in the organisation.

### The BC Strategy Implementation Metrics shall be used to measure the success of the BCprogramme.

## The BCM Implementation

### BCM shall be conducted in accordance with the BCM framework.

### BCM Awareness campaigns shall be carried out twice per annum, including the regional offices.

### BCM in the organisation shall conduct regular tests as and when required or planned by the BC Committee.

### The Disaster Recovery site shall be prepared by the Disaster Recovery Committee during tests before the [Department] official can occupy the site.

### Transport to the disaster recovery site shall be made available for all relevant employees.

### 

### BC tests conducted shall not disrupt the normal day-to-day operations of the [Department].

### 

### Business Units shall review their BC plans on a regular basis or as required by the [Department] management.

### BC test results shall be monitored, evaluated and the impact recorded and reported to the BC committee and the DG.

### BC exercise planning shall be prepared and finalised a week in advance.

### Employees shall be made aware of assembly points prior to BC tests in order to avoid confusion, should a disaster occur.

### Post exercise audits, shall be carried out by the internal audit unit.

## Reporting

### The BC committee shall agree on reporting intervals for all BCM activities with the relevant committees and the Recovery Coordinator.

### The Recovery Coordinator shall report to the BC committee as per the agreed time frame.

### The BC committee shall report on a quarterly basis to the Risk Committee and the DG.

5.6 The [Department] shall outsource and insource IT activities to service providers and other short-term activities to qualified contractors.

5.7 The Disaster recovery site shall be outsourced to Business Continuity SA to mitigate foreseeable cases of disruptions.

5.8 BCM in the [Department] shall be structured from the strategic level of the business through the BCC to carry out the activities on behalf EXCO, and then it cascades to the tactical level through coordination and support from three committees, namely: SHERQ, the Business Recovery Committee and the Disaster Recovery Committee.

5.8 At an operational level the latter committees shall consist of teams and/or groups that implement the activities of BCM in the [Department].

5.10 This is the environmental basis from which the entire BCM scope shall consider, ponder and subvert disaster strikes that can hamper the functions of the [Department].

# Limitations and conditions

6.1 The Business Continuity Management Policy applies to all [Department] employees without exception including, permanent and contract employees, and is also applicable to suppliers and vendors.

6.2 Non adherence to the Business Continuity Management Policy instructions shall amount to misconduct.

# Roles and responsibilities

## The BC Committee is responsible for:

### constituting the subcommittees, namely: SHERQ, Business Recovery, DR and Damage assessment;

### the authority to declare the state of emergency and disaster and to give relevant emergency instructions to all [Department] employees;

### implementing and maintaining the BCM policy and strategy;

### maintaining a high level BCM coordination within the [Department];

### storing all BC documents in a central location according to the National Archives standards;

### participating in all BCM programme activities;

### facilitating the BC programme management lifecycle and drafting documents through the Strategy and Policy unit;

### overseeing the activities of tactical level committees; and

### providing the BIA and CRA for the [Department].

## The Business Recovery Committee is responsible for:

### highlighting all circumstances that may disturb the institutional operations;

### manifesting resilience during any operational disruption;

### participating in the entire BCM programme implementation; and

### conducting business recovery tests according to plans.

## The SHERQ Committee is responsible for:

### facilitating evacuation, safety and wellness of employees;

### ensuring adherence to the OHS Act;

### reporting to the BCC during a disaster;

### reporting to the BCC in terms of evacuation plans and readiness;

### implementing the BCM programme at operational levels of the institution;

### identifying all physical threats that can hamper the institution’s facilities and security; and

### assisting the BC committee in creating staff awareness on the BCM programme.

### 

## The Disaster Recovery Committee is responsible for:

### reacting to business requests for technology and systems in times of incidents and emergencies;

### reporting to the BCC in times of a disaster;

### reporting to the BCC in terms of DR plans and readiness;

### maintaining ICT equipment that will assist the BCC in times of a disaster;

### identifying and maintaining disaster recovery sites; and

### arranging a disaster recovery team.

## Supply Chain is responsible for:

### providing emergency supplies in the disaster or incident;

### mandating suppliers to have a BC plan in place;

### providing the BC committee with updates regarding the [Department]’s outsourced activities; and

### participating in the BCM programme.

## The Legal Services division is responsible for:

### providing legal opinions; and

### participating in the BCM programme.

## The Risk and Audit unit is responsible for:

### reviewing all BC plans in all levels – strategic, tactical, and operational level; and

### coordinating with all [Department] divisions and stakeholders in evaluating risks for BCM purposes.

## The Communication unit is responsible for:

### [Department] and Customer reputation management;

### drafting a communication strategy for BCM programme; and

### communicating with management and staff on BCM issues during a declared disaster.

## The Corporate Monitoring and Evaluation unit is responsible for:

### monitoring Adherence to BC good practice guidelines;

### monitoring and reporting post incidents and tests; and

### evaluating according to BC good practice guidelines.

## The Internal Audit unit is responsible for:

### post exercise audits.

# Concluding comments

## This policy is a directive and subject to change and verification. Employees of the [Department] must be made aware of this policy together with its associated procedures and processes. The policy shall be reviewed as and when required; or when a need to add / change arises on legislation or procedures.

# Document Reference Library

|  |  |
| --- | --- |
| **Document File Name** | **Context and Relevance** |
| Business Continuity Management policy | The Business Continuity Management Policy for [Department] seeks to outline and steer the institution’s disaster management capability - through promoting resilience, efficient recovery, and foreseeing high risks that can reduce the institution’s abilities to deliver services |

# Business Areas impacted by this Policy

|  |  |
| --- | --- |
| **Name of Business Unit / Area** | **Context and Relevance** |
| All [Department] employees, contractors, clients, and all stakeholders | Every juristic and natural person interacting with and within the institution for the purpose of providing services to clients |

# Regulatory Framework

|  |  |
| --- | --- |
| **Statute / Policy / Regulation** | **Applicability** |
| Constitution of the Republic of South Africa Act No. 108 of 1996 | The supreme law of the land. |
| Occupational Health and Safety Act as amended by Occupational Health and Safety Amendment Act (No. 181 of 1993) | To provide for the health and safety of persons at work and for the health and safety of persons in connection with the use of plant and machinery; the protection of persons other than persons at work against hazards to health and safety arising out of or in connection with the activities of persons at work |
| Batho Pele Principles | Meaning ‘People First’, it highlights the importance of treating clients well in order to attain effective service delivery. |
| ISO 22301 |  |
| King VI codes of Corporate Governance | Prescribe the importance of implementing Business Continuity in an institution to enhance corporate performance |
| PFMA (Public finance management) Act of 1999 | Framework for guiding public institutions’ financial accountability and integrity |
| National Archives and Record Service of South Africa act of 1996 | Provides standards and systems for filing documents in South African Public institutions |
| Business Continuity Institute :Good Practice Guidelines | Provides management guidelines in order to ensure the implementation of good global BC guidelines. |

# Descriptions of Abbreviations and Concepts

|  |  |
| --- | --- |
| **Abbreviations** | **Description** |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
| **Concepts** | **Description** |
| Activities | All duties that belong to the business means of operations. |
| BCM Programme lifecycle | The processes and systems of practicing Business Continuity in an institution |
| Disruption | A disturbance of any nature within [Department] that can critically hamper the delivery of services |
| Emergency | A serious situation or occurrence that happens unexpectedly and demands immediate action |
| Employee | Any person, excluding an independent contractor, who works for another person or for the State and who receives, or is entitled to receive, any remuneration; and,  Any other person who in any manner assists in carrying on or conducting the business of an employer, and 'employed' and 'employment' have meanings corresponding to that of ‘employee'. |
| Foreseeable threats | Only threats that can be outlined by using BCM good practice tools |
| Good Practice | Mechanisms and tools for BC management provided by the Business Continuity Institute’ Good Practice Guidelines |
| Misconduct | unacceptable or improper behaviour, especially by an employee or professional person |
| Mission Critical Activities | Operational duties of the institution which are indispensable in order to provide services to clients. e.g. Call Centre |
| Multi-Activity | The integration of activities – transactions between [Department] and its stakeholders, clients, and contractors |
| National Archives Standards | Set of rules on the implementation of file numbering system |
| Recognised DBC Unions | Trade Union recognized by the DBC |
| Resilience | The institutions ability to remain calm during an incident or disaster and still operate normally |
| Stakeholders |  |
| Tests | Staged activities conducted to ensure that risk mitigating measures that are put in place are working and will work in an instance where the actual risk occurs. |