



**DRAFT BUSINESS CONTINUITY STRATEGY – 2023/2024**

## Table of Contents

|                                                                     |           |
|---------------------------------------------------------------------|-----------|
| <b>1. Purpose, scope, and users .....</b>                           | <b>2</b>  |
| <b>2. Reference documents.....</b>                                  | <b>2</b>  |
| <b>3. Recovery Strategy.....</b>                                    | <b>2</b>  |
| 3.1. Strategy input .....                                           | 2         |
| 3.2. Business Impact Analysis.....                                  | 2         |
| 3.3. Risk management.....                                           | 2         |
| 3.4. 3Detailed Strategy .....                                       | 3         |
| <b>4. Incident response structure.....</b>                          | <b>3</b>  |
| 4.1. Crisis Management Team and Crisis Management Support Team..... | 3         |
| 4.1.1. Crisis Management Team .....                                 | 3         |
| 4.1.2. Crisis Management Support Team.....                          | 3         |
| 4.1.3. Command Centre Equipment.....                                | 4         |
| 4.2. Reporting and decision making .....                            | 5         |
| 4.3. Cooperation with authorities .....                             | 6         |
| 4.4. Building evacuation and assembly points.....                   | 6         |
| 4.5. Means of communication .....                                   | 6         |
| 4.6. Transportation to alternative sites.....                       | 6         |
| 4.7. Communicating with interested parties and community .....      | 7         |
| <b>5. Resource Strategy .....</b>                                   | <b>7</b>  |
| 5.1. Sites and infrastructure .....                                 | 7         |
| 5.2. Suppliers and outsourcing partners.....                        | 7         |
| 5.3. Applications/databases.....                                    | 8         |
| 5.4. Data .....                                                     | 8         |
| 5.5. Avoiding a single point of failure.....                        | 8         |
| 5.6. Providing financial resources.....                             | 8         |
| <b>6. Recovery strategy for individual activities .....</b>         | <b>8</b>  |
| <b>7. Implementing all necessary preparations.....</b>              | <b>8</b>  |
| <b>8. Managing records kept based on this document.....</b>         | <b>8</b>  |
| <b>9. Validity and document management.....</b>                     | <b>9</b>  |
| <b>10. Appendices.....</b>                                          | <b>9</b>  |
| <b>11. Concluding Comments.....</b>                                 | <b>9</b>  |
| <b>12. Glossary of Terms .....</b>                                  | <b>9</b>  |
| <b>13. Acknowledgement of Approval.....</b>                         | <b>11</b> |

## **1. Purpose, scope, and users**

Business continuity management deals with the analysis, design, and implementation of policies, plans, and procedures that address all aspects of a municipality's ability to survive and continue operations during a crisis. The purpose of this document is to define how Langeberg Municipality will ensure that all conditions for the resumption of business activities in the case of disaster or other disruptive incident are met. It forms the basis for preparing the Business Continuity Plan and recovery plans. This document is applied to the entire BCM scope as defined in the Business Continuity Management Policy. Users of this document are members of strategic management team, business continuity committee and other persons implementing the business continuity management of the municipality.

## **2. Reference documents**

- ISO 22301:2019 standard
- Business Continuity Management Policy
- Business Impact Analysis questionnaires
- Risk Assessment Report
- Business Continuity Plan containing the Incident Response Plan and recovery plans.
- Business Continuity Implementation Plan

## **3. Recovery Strategy**

### **3.1. Strategy input**

This Strategy is written based on Business Impact Analysis results and results of risk assessment and risk treatment.

### **3.2. Business Impact Analysis**

The Business Impact Analysis should establish activities that support key business processes for service delivery. A list of such activities should be compiled and appended to this strategy.

The maximum tolerable period of disruption (maximum acceptable outage) for each activity should be determined in the Business Impact Analysis Questionnaire and appended to this strategy for activity recovery strategy.

The recovery time objectives for each activity should be determined, considering dependencies on other activities, and appended to this strategy.

### **3.3. Risk Management**

Assessment of risks which could affect business continuity should be described in a Risk Assessment Report. The highest risks which could lead to a disruptive incident, i.e., business disruption should be identified during risk assessment, and it is necessary to for all mentioned risks / incidents to cover the following:

1. Preventive action applied to reduce the probability of such risks/incidents - the actions should be described and documented.
2. Preventive action applied to minimise possible consequences of such risks/incidents - these actions should also be described and documented.
3. Event/incident scenarios which describe how such incidents could affect the organization's operations should be prepared and appended to this strategy and must be used at a later

point for testing plans.

4. Define in the Incident Response Plan the appropriate way to respond to each of the incidents/risk.

### **3.4. Detailed Strategy**

The existing business continuity strategy of Langeberg Municipality is limited to information technology service continuity for critical activities. It did not cover enterprise-wide business continuity covering manual and automated, technological, and non-technological critical activities of the municipality. A detailed business continuity plan for the entire municipality should be developed and implemented.

## **4. Incident response structure**

### **4.1. Crisis Management Team and Crisis Management Support Team**

#### **4.1.1. Crisis Management Team**

If business continuity plans are activated, a working body called Crisis Management Team is formed which is authorised to make any decisions to resolve the situation. Members of the Crisis Management Team are all members of the Strategic Management Team (SMT), chaired by the Municipal Manager or delegated SMT member in cases where the Municipal Manager is not available. The Municipal Manager shall be the Crisis Manager. The Crisis Management Team manages the disruptive incident from a facility called the Command Centre, the location of which is specified in item 5.1 of this strategy.

#### **4.1.2. Crisis Management Support Team**

The Crisis Management Support Team has the function of relieving the Crisis Management Team from administrative and other operational activities, to focus on managing the disruptive incident.

Members of the Crisis Management Support Team are:

- Person from the communications department
- Person from the human resources department
- Person from the disaster management department
- Person from the supply chain management department
- Person from the traffic, law enforcement and security department
- Health and safety representative
- Business Continuity Coordinator
- Person from the ICT department
- Any other member of the Operational Management Team (OMT) deemed necessary by the Crisis Management Team to provide support.

The Crisis Management Support Team shall work on locations specified by the Crisis Management Team. The Crisis Management Team may allocate tasks to any member of the Crisis Management Support Team individually or collectively with other members depending on the crisis at hand or the necessary expertise required to manage the crisis.

#### 4.1.3. Joint Operations Centre Equipment

To serve the Crisis Management Team and Crisis Management Support Team the Joint Operations Centre at the Robertson Fire Station must be equipped as follows:

| Name of resource                                                   | When the resource is necessary |
|--------------------------------------------------------------------|--------------------------------|
| <b>Applications / databases:</b>                                   |                                |
| Financial System                                                   | Immediately                    |
| Procurement System                                                 | Immediately                    |
| Payment System                                                     | Immediately                    |
| <b>Data stored in electronic form:</b>                             |                                |
| Business Continuity Management Policy                              | Immediately                    |
| Business Continuity Strategy and plans for all critical activities | Immediately                    |
| Contingency plans of all critical activities                       | Immediately                    |
| <b>Data stored on paper:</b>                                       |                                |
| Business Continuity Management Policy                              | Immediately                    |
| Business Continuity Strategy and plans for all critical activities | Immediately                    |
| Contingency plans of all critical activities                       | Immediately                    |
| <b>IT and Telecommunications equipment:</b>                        |                                |
| Desktop PC Workstations                                            | Within 2 hours                 |
| Laptops                                                            | Immediately                    |
| Telephones                                                         | Immediately                    |
| Mobile phones                                                      | Immediately                    |
| Printer                                                            | Within 2 hours                 |
| Fax machine                                                        | Immediately                    |
| <b>Communication channels:</b>                                     |                                |
| Telephone land lines                                               | Immediately                    |
| Internet access - Emails, social media etc.                        | Within 2 hours                 |
| <b>Other equipment:</b>                                            |                                |
| TV set                                                             | Immediately                    |
| Radio                                                              | Immediately                    |

| <b>Facilities and infrastructure:</b> | <b>When the resource is necessary</b> |
|---------------------------------------|---------------------------------------|
| Computer network                      | Within 2 hours                        |
| Furniture                             | Immediately                           |

| <b>External services:</b>                         | <b>When the resource is necessary</b> |
|---------------------------------------------------|---------------------------------------|
| Electricity                                       | Immediately                           |
| Alternative energy supply i.e., generators or UPS | Within 4 hours                        |
| Fuel                                              | Within 2 hours                        |

The Crisis Manager, assisted by the BCM Administrator, is responsible for preparing the Crisis Management Team and the Crisis Management Support Team for their role during a disruptive incident. The Crisis Management Team is responsible for equipping the Joint Operations Centre. The Crisis Manager can direct any member of the Crisis Management Team and/or the Crisis Management Support Team to assist with equipping the Joint Operations Centre.

#### **4.2. Reporting and decision making**

Disruptive incidents should be reported in the following ways:

- All incidents related to Information and Communications Technology (ITC) are reported to ICT Manager.
- All other incidents are reported to the responsible member of the Operational Management Team (OMT).

If the persons responsible are unable to resolve the incident, they must inform the Crisis Manager who decides whether to activate recovery plans.

Authorisations for making decisions are the following:

| <b>Type of decision</b>                                                             | <b>Who is authorised</b>                                |
|-------------------------------------------------------------------------------------|---------------------------------------------------------|
| How small incidents related to IT and communications technology are resolved        | Employees in ICT Department                             |
| How all other small incidents are resolved                                          | Relevant OMT Member                                     |
| Deciding about activating recovery plans                                            | Crisis Manager                                          |
| Implementing all tasks necessary for the recovery of individual critical activities | Relevant OMT member                                     |
| Selecting information to be provided to the public media during disruptive incident | Crisis Manager in consultation with the Executive Mayor |
| Purchases during disruptive incident - over R20 000                                 | Crisis Manager or delegated member of the SMT           |
| Purchases during disruptive incident - up to R20 000                                | Responsible manager                                     |

The ICT Manager is responsible for preparing employees in the ICT department to recognise and react to incidents related to IT and communications technology. The relevant manager is responsible for preparing employees in their respective department to handle other incidents.

#### 4.3. Cooperation with authorities

The following persons oversee coordination with state authorities and emergency services:

| Authority                                              | Who is responsible                                         |
|--------------------------------------------------------|------------------------------------------------------------|
| Police, Law Enforcement, Security and Traffic Services | Director - Corporate Services                              |
| Ambulance Services                                     | Director – Community Services and/or Chief Fire & Disaster |
| Fire and Disaster Service                              | Director – Community Services and/or Chief Fire & Disaster |
| Any others                                             | Responsible SMT member                                     |

The mentioned persons should implement all preliminary activities to ensure interoperability with authorities during disruptive incident is at a satisfactory level. Preliminary activities may include obtaining instruction from authorities regarding the type of information required in the case of disruptive incident and how the municipality is expected to react.

#### 4.4. Building evacuation and assembly points

The evacuation plans and procedures of each building/facility/plant should be developed and documented as required by occupational health and safety act and other relevant prescripts in case fires or other health emergencies. The evacuation plans and procedures should make provision of assembly points.

#### 4.5. Means of communication

The following means of communication will be used in the case of disruptive incident – those at the top of the list are to be used first, those near the bottom are used only if the former are out of order:

1. Mobile phones
2. Telephones
3. E-mail
4. Messaging services - e.g., Langeberg Municipality Website, Facebook, Skype, MS Teams, WhatsApp, X (Twitter)
5. Couriers (employees of the municipality or specialised services)
6. Radio stations
7. Satellite phones –

The Manager IDP, PMS and Communications, with the support of Manager ICT, is responsible for acquiring/preparing and when necessary, maintaining the mentioned means of communication to ensure they are available during a disruptive incident.

#### 4.6. Transportation to alternative sites

Employees of the municipality will be transported from the primary to the alternative site in the following ways:

| Activity                                                  | Means of transport                                                                      |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------|
| Crisis Management Team and Crisis Management Support Team | On foot; by private car; by business car; by rented bus; or using public transportation |

The municipal wide business continuity plans should provide for all means of transportation for employees for all critical activities. A scenario-based transportation should be developed as part of the municipal wide business continuity plans.

#### **4.7. Communicating with interested parties and community**

The communications department or any other person so designated should handle relations with interested parties and wider community on instruction of the Crisis Manager and the Executive Mayor in the case of a disruptive event.

### **5. Resource Strategy**

#### **5.1. Sites and infrastructure**

The municipal wide business continuity plan should make provision for recovery sites of considering the following:

- Primary site
- Alternative site
- Number of workplaces
- Equipment required per site.
- Joint Operations Centre
- Alternative sites that can be provided by an associate organisation (
- Reciprocal contracts (if there are organisations using the site of the same or similar configuration and infrastructure, they can arrange a contract according to which an organization gives /rents its site and infrastructure to another organization in the case of disaster)
- Alternative sites provided by specialised organisations (e.g., organizations which rent their facilities for the case of disaster, but also hotels or, for example, educational institutions equipped with ICT infrastructure)
- Working at home or at some other remote location

The Crisis Manager, assisted by the Crisis Management Team, is responsible for making all necessary arrangements concerning alternative sites.

#### **5.2. Suppliers and outsourcing partners**

Relations with suppliers and outsourcing partners should be managed in the following ways:

- Services are contracted from several suppliers or outsourcing partners simultaneously – if one partner is unavailable, the services of another can be used (E.g., The tenders should be awarded to alternative bidders in order of preference should the preferred bidder fail deliver in terms of the contract.)
- Service level agreements with suppliers should ensure that they raise their level of business continuity capability to reduce the risk of an incident and reduce its consequences.
- Obliging the suppliers/outsourcing partners by contract to deliver the product or service regardless of the disruptive incident and define penalties. In this way suppliers/outsourcing partners are obliged to introduce business continuity and transferring a part of the financial risk to them.
- Alternative suppliers or outsourcing partners should be defined. In this way the transfer of business can be prepared, although the business relationship does not start until a disruptive incident occurs.
- Return of activities back to the municipality, preparing the municipality to take over activities that have been outsourced.



### 5.3. Applications/databases

All the necessary applications and databases should be installed at the alternative site if they are required within 24 hours from disruptive incident; for those applications and databases which are not required within 24 hours, the installation media should be stored at the alternative site.

### 5.4. Data

Backup copies of data should be installed and shared by several critical activities as and when required for business continuity purposes as stipulated in the disaster recovery strategy and plan of the municipality.

### 5.5. Avoiding a single point of failure

Strategies should be developed and documented for implementation to avoid a single point of failure which can cause a disruption of a critical activity.

### 5.6. Providing financial resources

Langeberg municipality should determine how much is required for working capital for all critical activities, and for urgent purchases in case a disruptive incident. The required financial resources should be continuously maintained at the required level of liquidity in money; and a stand-by arrangement with a financial institution, where required. Suppliers be encouraged to extend the payment terms in case of a disruptive event. Disaster and/or emergency funds should be sourced from disaster/emergency funds available at district, provincial or national government where applicable.

## 6. Recovery strategy for individual activities

The recovery strategy for individual activities should defined in the Activity Recovery Strategy for each department. The manager of each department is responsible for writing Recovery Plans for each critical activity in their respective departments.

## 7. Implementing all necessary preparations

All necessary preparations for the implementation of this strategy should be documented in a Preparation Plan for Business Continuity and appended to this strategy. The Chief Audit Executive must define the necessary financial and other resources and set deadlines for the implementation of each preparation; and should monitor the coordination and execution of all preparatory actions, as well as of reporting about their implementation.

## 8. Managing records kept based on this document

| Record name                                       | Storage location           | Person responsible for storage | Control for record protection                                                                                                                    | Retention time                                                                                                    |
|---------------------------------------------------|----------------------------|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Business Continuity Strategy (in electronic form) | Internal Audit share drive | Chief Audit Executive          | Only Chief Audit Executive has the right to make entries and changes to this strategy, after consultation with the Business Continuity Committee | The Strategy will be stored and retained according to records management and archives policy of the municipality. |

## 9. Validity and document management

This document is valid from the date approval and should be reviewed for updates at least once a year. When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

- whether the municipality succeeded in recovering activities within the recovery time objective, and
- whether all necessary preparations for business continuity have been implemented.

## 10. Appendices

The following documents should be developed and appended to this strategy:

- Appendix 1 - List of Critical Activities
- Appendix 2 - Recovery Priorities for Critical Activities
- Appendix 3 - Recovery Time Objectives for Critical Activities
- Appendix 4 - Examples of Disruptive Incident Scenarios
- Appendix 5 - Preparation Plan for Business Continuity
- Appendix 6 – Scenario Based Activity Recovery Strategy for each Department

## 11. Concluding Comments

This document shall be known as the Business Continuity Strategy. Employees of the municipality must be made aware of this strategy together with its associated procedures and processes. The strategy shall be reviewed as and when required; or when a need to add / change arises on legislation or procedures. This strategy shall be effective until a new one has been approved.

## 12. Glossary of Terms

| Term/Concept/Abbreviation | Description                                                                     |
|---------------------------|---------------------------------------------------------------------------------|
| BCM                       | Business Continuity Management                                                  |
| BCC                       | Business Continuity Committee                                                   |
| BC                        | Business Continuity                                                             |
| Standards                 | International Standards for the Professional Practice of Internal Auditing      |
| SMT                       | Strategic Management Team                                                       |
| OMT                       | Operational Management Team                                                     |
| FARMCO                    | Fraud and Risk Management Committee                                             |
| A&PC                      | Audit and Performance Committee                                                 |
| Activities                | All duties that belong to the business means of operations.                     |
| BCM Program lifecycle     | The processes and systems of practicing Business Continuity in the municipality |

|                     |                                                                                                                                                                                                                                                                                                                                                |
|---------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Disruption          | A disturbance of any nature within the municipality 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 the municipality and who receives, or is entitled to receive, any remuneration; and,<br>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                                                                                                                                                                                                                                                           |
| Critical Activities | Operational duties of the municipality which are indispensable in order to provide services to the public. e.g. Call Centre.                                                                                                                                                                                                                   |
| Multi-Activity      | The integration of activities – transactions between municipality and its stakeholders, clients, and contractors                                                                                                                                                                                                                               |
| Resilience          | The municipality's ability to remain calm during an incident or disaster and still operate normally.                                                                                                                                                                                                                                           |
| 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.                                                                                                                                                                               |
| ICT                 | Information and Communication Technology                                                                                                                                                                                                                                                                                                       |

**Compiled by:**

Ayanda Mati  
Chief Audit Executive

---

1 March 2024

### 13. Acknowledgement of Approval

Approved by the Municipal Manager:

Position: Municipal Manager (Business Continuity Committee Chairperson)

Signature: \_\_\_\_\_

Name in Print: \_\_\_\_\_

Date: \_\_\_\_\_