**BELA-BELA LOCAL MUNICIPALITY**

Chris Hani Drive, Bela- Bela, Limpopo. Private Bag x 1609
BELA-BELA 0480
Tel: 014 736 8000 Fax: 014 736 3288
Website: www .belabela.gov.za

**OFFICE OF THE MUNICIPAL MANAGER**

# Information and Communication Technology

# Service Continuity Plan

**DOCUMENT AUTHORITIES**

| | |
|---|---|
| Compiled by | |
| Designation | |
| Signature | |
| Date | |
| Approved by | |
| Supported by | |
| Designation | |
| Signature | |
| Date | |
| Approved by | |
| Designation | |
| Signature | |
| Date | |
| Effective date | From date of approval |

# 1. Introduction

## 1.1 Policy Development

The realisation of this policy is a direct reflection of Bela-Bela Local Municipality's commitment to implementing an IT Disaster Recovery (also referred to as an IT Continuity) Plan under the umbrella of Business Continuity Management (BCM) at a level that would be independently acknowledged to be compliant with international best practice.

## 1.2 Definition of BCM and IT Continuity Management

BCM and IT Continuity Management is the strategic and tactical capability of the Municipality to plan for and respond to major incidents and internal business disruptions in order to continue business and IT operations at an acceptable pre-defined level.

## 1.3 Organisational position of IT Continuity Management

Bela-Bela Local Municipal Council remains accountable for the implementation of IT Continuity Management, consistent with its responsibility for the total process of risk management and internal control.

## 1.4 Scope

This policy applies to all Bela-Bela Local Municipality site offices, facilities and IT systems at all locations. The Municipality will be prepared for and develop an effective response to scenarios including, but not limited to, natural disasters, power outages, Information Technology hardware / telecommunications failures, loss of premises, loss of data centre or computer room, criminal activity, fires, civil and industrial unrest etc.

In terms of our commitment to the protection and preservation of skills, assets and our reputation, emergency response (such as a building evacuation and staff safety) falls under the Occupational Health and Safety function in Municipalities, and crisis management (such as dealing with the media) will be deemed to form part of the Communications Section.

BCM and IT Continuity Management awareness will be incorporated into staff induction courses.

# 2. IT Service Continuity Management Objectives

## 2.1 Goal of IT Service Continuity in the Municipality

This policy provides guidance for the Resumption and Recovery of time sensitive business operations and critical ICT infrastructure in accordance with pre-established timeframes as well as ensuring that adequate plans are in place for the less time sensitive business operations.

IT Service Continuity will be developed and implemented to ensure the municipality can withstand a severe business or IT disruption which has the potential to prevent the municipality from supplying essential services and billing processes which are critical to the survival of the business.

### 2.2 Methodology

IT Service Continuity Management development, implementation, strategy and maintenance will be compliant with British Standards BS 25999:2006 Parts 1 and 2, together with BS 25777:2008. The methodology also aligns with and conforms to the London based Business Continuity Institute (the BCI) Good Practice Guidelines publication, which was a significant contributor to BS 25999 and BS 25777.

IT Service Continuity implementation will be based on business driven requirements, and therefore certain elements of Business Continuity Management will be used, namely a Business Impact Analysis and an operational Risk Analysis / Assessment.

### 2.3 Worst Case Scenario

In keeping with accepted international best practice, IT Service Continuity will cater for total loss of strategically important premises, the total loss of technology, loss of key staff, or all of the above.

IT Service Continuity will be implemented with due regard to the acknowledgement that such catastrophic events may incur casualties and loss of life.

### 2.4 IT Continuity Management Starting Points

IT Continuity implementation will commence with the clear assignment of responsibilities, the preparation of a project charter and project plan, training and awareness and the approval of budget.

### 2.5 Relevant Legislation and Regulation

Developed IT Service Continuity plans and solutions will take into account the relevant provisions of the Occupational Health and Safety Act, as well as the relevant governing portions of the following:

- SITA Act (Act No. 88 of 1998)
- SITA Amendment Act (Act No. 38 of 2002)
- NIA Minimum Information Security Standards
- National Strategic Intelligence Act (Act No. 39 of 1996)
- Protection of Information Act (Act No. 84 of 1992)
- Promotion of Access to Information Act (Act No. 2 of 2000)
- Interception and Monitoring Bill (B50 – 2001)
- Electronic Communications and Transactions Bill (B8 – 2002)
- Public Service Act (Act No. 104 of 1996)
- Labour Relations Act (Act No. 12 of 2002)
- Copyright Act (Act No. 88 of 1978)
- National Archives of South Africa Act (Act No. 43 of 1996)

## 3. IT Continuity Management Control Process

### 3.1 Process Organisation

Bela-Bela Local  Municipality IT Steering Committee will appoint an IT Continuity Plan Management Team and an IT Continuity Coordinator and deputy. When full BCM is implemented a Business Continuity Coordinator will be required, and the IT Continuity Coordinator may then assume this role. IT Continuity (Disaster Recovery) teams will be identified to assume responsibility for the recovery of all critical technology infrastructure (including total loss of data centres) that support identified mission critical activities (business processes). All team leaders will be deputized.

### 3.2 General BCM Process Requirements

The outcome of a developed BCM solution will be Business Continuity Plans for all mission critical activities, Information and Communication Technology enabling systems, Crisis Management and Emergency Response Plans, as well as a tested off-site recovery capability. IT Continuity (Disaster Recovery) Plans based on a business impact analysis and risk assessment will be developed first, during Q1 and Q2 2011.

### 3.3 Maintenance, Test and Audit

The developed IT Continuity (IT Disaster Recovery) solution will be maintained (in perpetuity) in a fully deployable capability in terms of a maintenance strategy which will be signed off by the Management Committee.

Testing of system and process recovery will occur at least once per annum, and will be subjected to the scrutiny of external and internal auditors as and when required. Change Control will be amended to incorporate IT Continuity Management and BCM requirements. Strategy, plans and associated solutions will be re-evaluated and updated annually, and whenever there is a significant change in technology, premises, personnel, process, market, or organisational structure.

### 3.4 Compliance with IT Continuity Management Policy

All employees of the Bela-Bela municipality are required to comply with this policy and a signed copy of this policy will be filed with relevant personnel records.

All accountable and responsible BCM role-players will be subject to regular appraisals in terms of existing Key Performance Indicators.

### 3.5 Evaluation and Maintenance of IT Continuity Management Policy

Ownership of this Policy shall be vested with Municipal Management who will review the document on a regular basis (at minimum) annual basis.

### 3.6 Outsourcing

All companies deemed to be critical to Bela-Bela Local Municipality’s supply chain will be encouraged to employ similar standards of Business Continuity Management / IT Continuity Management.