ITEM A-CORP (12-2017) OC: CM 26/10/2017	BUSINESS CONTINUITY MANAGEMENT POLICY OF THE CITY OF EKURHULENI

RESOLVED

1. **That** the Corporate & Shared Service Oversight Committee report on Risk Management's request for the approval of the business continuity management policy of the City of Ekurhuleni **BE NOTED**.

2. **That** all Councilors BE WORKSHOPPED on the Business Continuity Management Policy by the end of the 3rd quarter of the 2017/2018 financial year.

BUSINESS CONTINUITY MANAGEMENT POLICY

EFFECTIVE DATE: OCTOBER 2017

Table of Contents

1.   Introduction

1.1.   Business Continuity Management (BCM) is a key performance area within the Business Risk division within the EMMs Risk Management Department. The BCM Programme is an organisation-wide response to the risk of disruption of the urgent (mission critical) processes as a result of a variety of causes, factors and circumstances. The implementation of the BCM Programme will enable departments to not only maintain some level of business operations for critical processes in the event of a disruption to normal operations, but to also, resume normal business processes as effectively as possible.

1.2.   The EMM is faced with significant challenges relating to unemployment and economic development, as well as the provision of basic services such as water, sanitation, electricity, housing, health services, education, safety and economic development. It is the EMMs Policy to conduct its operations with the highest regard for the safety and health of its employees and the public, and for the protection and preservation of property and the environment. Continuity of business operations must be maintained, and the interests of stakeholders protected, even under the most adverse circumstances. It is therefore vital that the EMM has practical and robust Business Continuity Plans (BCPs) which will serve to protect the community and all interested stakeholders, during any major threat or incident, through its timely and orderly recovery.

1.3.   The BCM programme aims to improve EMMs urgent strategic, tactical and operational business processes to a *resilient* state of functionality to enable efficient and reliable service delivery.

1.4.   Resilience is widely defined as *"the ability of an organisation to absorb, respond to and recover from a disruption".*

   "BCM is defined as a holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities." (Source: ISO 22301:2012)

1.5.   EMM's Business Continuity (BC) Programme identifies and evaluates risks to its assets and operations, maintains prevention procedures and mitigates the effects of unforeseen losses by having in place processes of continuity and recovery that are regularly audited, tested and updated.

1.6.   More specifically, the BC programme will cover:
   * Descriptions of Emergency Response, Crisis Management and Business Recovery, dealing with notification procedures and internal/external interfaces.
   * Training requirements.
   * Maintenance and testing of plans and procedures once they are developed.

2.   Approach and Methodology

Good Practice Guidelines (GPG: 2013) and ISO 22301:2012 methodologies were employed in the development of EMMs Business Continuity Management System (BCMS)

The GPG BCM Lifecycle comprised of six (6) professional practices which were derived from the ISO 22301 standard. The diagram below depicts the BCM lifecycle:

Policy and Programme Management
- Is the Professional Practice at the start of the Business Continuity Management (BCM) Lifecycle. It is the Professional Practice that defines the organizational policy relating to Business Continuity (BC) and how that policy will be implemented, controlled and validated through a BCM program.

Embedding Business Continuity
- Is the Professional Practice that continually seeks to integrate BC into day-to-day business activities and organizational culture,

Analysis
- is the Professional Practice within the BCM Lifecycle that reviews and assesses an organization in terms of what its objectives are, how it functions and the constraints of the environment in which it operates.

Design
- is the Professional Practice within the BCM Lifecycle that identifies and selects appropriate **strategies** and tactics to determine how continuity and recovery from disruption will be achieved.

Implementation
- is the Professional Practice within the Business Continuity Management (BCM) Lifecycle that executes the agreed strategies and tactics through the process of developing the Business Continuity Plan (BCP).

Validation
- Is the professional practice that validates and confirms that the business continuity strategies are effective by means of testing, review and maintenance.
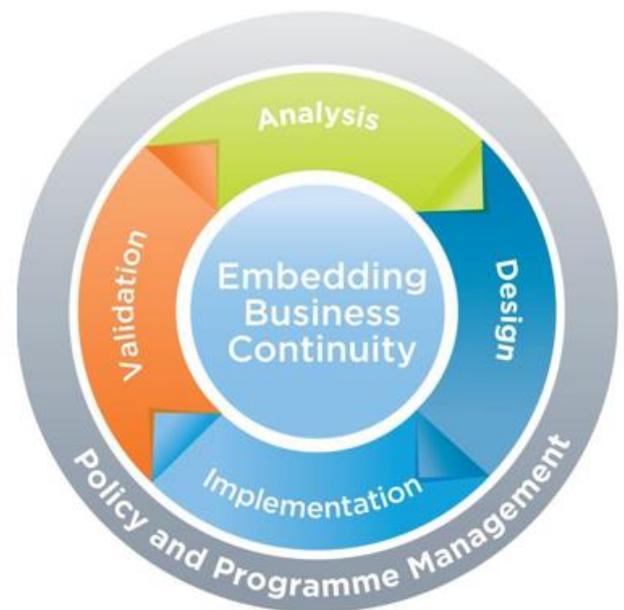
BCM Life Cycle GPG: 2013

BCM includes the continuous Business Continuity Institute (BCI) cycle of:
➢ Developing and adoption of a Policy and Programme management
➢ Embedding Business Continuity in means of Awareness programmes
➢ Understanding the organisation through conduction Business Impact Analysis reports and Risk Assessments
➢ Establishing a suitable BCM strategy in the Design phase of the cycle
➢ Developing and Implementing a BCM response in the form of BCPs
➢ Exercising, maintaining and reviewing BCM arrangements

To ensure that BCM processes are followed to achieve the objectives set out in this policy, a BCM programme has been adopted. The programme details the activities that are involved in each of the professional practices of the BCM lifecycle and groups them in pillars which are essentially EMMs key performance indicators and ultimately BCM enablers are detailed in the sections that follow.

3. Governance

The Business Continuity Policy sets the direction and approach for Business Continuity in EMM.

EMM Systems and Operations will be identified and rated on a prioritised basis for Business Continuity purposes. Allocation of resources shall be influenced by priorities.

It is essential to ensure that the BCM programme will work, and for this to be achieved, BCM documentation must be regularly updated and tested. The EMM relies on all stakeholders to give this initiative their full support. To ensure the BCM Programme delivers an integrated process, EMM will continue to audit, test and benchmark performance in this area against best practice and require any new processes to include BCM in their procedures.

3.1 Policy Statement

The EMM recognises and appreciates the risk of disruption to its key and critical operations.

It is EMM's policy to:
- Reduce the probability and impact of disrupting incidents to its people, operations and services by applying suitable BC techniques and approaches to improve EMM's resilience and its ability to restore normality within a planned time frame (Recovery Time Objective);
- Establish and maintain a Business Continuity Management System (BCMS) that includes strategies, policies, procedures, assessments, impact analyses and other documents;
- Incorporate BCM initiatives in the day to day operations, functions and planning of all functions;
- Review and improve EMM's Business Continuity system regularly, to accommodate the organisation's dynamic nature; and
- Ensuring continuity of the critical processes to a predefined, acceptable level.

To achieve this, BCM as an essential part of its day- to- day operations.

3.2 Purpose and Objective

The Purpose of the Policy is for the Ekurhuleni Metropolitan Municipality to adopt a comprehensive business continuity management framework and approach, which will help in achieving the objectives set below.

The overall objective of the Business Continuity Programme is to provide for an orderly and timely recovery of critical business processes from a disaster or disruptive incident, with the aim of safeguarding the safety of employees/citizens, and avoiding or minimising damage to EMM's reputation and its ability to operate. This is achieved by:

- Defining courses of response actions;
- Identifying personnel to take responsibility for Emergency Response, Crisis Management, and Business Continuity actions;
- Identifying external support for sustaining business activities;
- Establishing alternative strategies to sustain business activities; and
- Specifying the steps to physical reinstatement and the path to achieve business recovery.

3.3 ICT and Service Continuity Committee

The BC Steering Committee is a Senior Management Team (SMT) structure responsible to provide strategic direction and oversight of the entire BC Programme. The Committee shall operate under a formal Terms of Reference.

3.4 Risk Committee and Audit Committee

The Risk Committee and Audit Committee shall review and oversee the overall BCM Programme as part of their broader risk management system oversight mandates.

3.5 Internal Audit

Internal Audit provides independent and objective assurance over the adequacy and effectiveness of business continuity management processes.

3.6 BCM Documentation review

Business Impact Analysis (BIA) Reports, Strategy reports and BCPs will be reviewed at least annually or shall also be reviewed in the event of significant changes in the environment. The strategies adopted should enable the continuation of critical processes within the recovery timeframes stipulated.

3.7 Policy Review

This policy shall be reviewed at least once every two years. The policy shall also be reviewed in the event of significant changes in the environment.

.

4. Resources

4.1 Scope of Application

The successful implementation of BCM within the EMM is dependent upon the commitment of the SMT. This Policy is applicable to EMM Departments, EMM Entities and its suppliers of essential services.

Events falling within the ambit of Disaster Management (as per the Act 57 of 2002) are not covered by BCM.

4.2 Roles and Responsibilities

The responsibilities of the key roles involved in the BC Programme are the following:

a) City Manager

The City Manager is the owner of Business Continuity in EMM and is ultimately accountable for BC in EMM.

The City Manager is accountable to the Council for designing, implementing and monitoring a Business Continuity Programme. The City Manager must:
- Ensure that the BC strategy is defined and adopted by management;
- Ensure that adequate structures are put in place to manage BCM.

b) Chief Risk Officer (CRO)

The CRO is the custodian of the BC Programme of the EMM and is responsible for.
- Developing an appropriate framework, including methodologies, tools and techniques, to facilitate the implementation of business continuity management processes;
- Facilitating BC awareness and processes in the EMM;
- Assuring that the required levels of BC readiness are maintained in their respective areas of responsibility, as well as the remainder of the company;
- Monitoring the BCM Programme;
- Reporting on the status of the BCM Programme to relevant stakeholders
- Arbitrating in critical BC issues when necessary;
- Conducting BC Steering Committee meetings;
- Delegating tasks stemming from the BC Steering Committee meeting to members and/or the Business Continuity function;
- Delegating the daily functions of Business Continuity to the BC function;
- Assuring that BC objectives and targets form an integral part of day to day operations;
- Provide assistance where needed during internal and external BCM audits; and
- Make recommendations toward the improvement of the BCMS including related policies, strategies and procedures.

c) Heads of Department (HoDs)

The HoDs are responsible to develop, maintain, exercise and execute the BCPs in their respective areas of responsibility. The HoDs are accountable for:
- Allocating resources to meet Business Continuity objectives and targets;
- Escalate any BC issues in their departments that may have an impact on EMM as a whole;
- Reviewing the effectiveness of the BCMS;
- Assure the BC readiness of the company and especially in their fields of responsibility;
- Allocating responsibility for Business Continuity processes within their departments;
- Regularly conducting Business Impact Analyses (BIA) on own systems, procedures and services at least annually;
- Determining and implementing appropriate actions to reduce BC risks;
- Designing and operating systems with resilience and ease of recovery in mind;
- Developing and implementing BCPs and procedures for identified critical systems and processes;

- Determine BC strategy for the EMM at Departmental level;
- Regularly exercising BCPs;
- Continuously improving the BCMS, documents, plans and initiatives; and
- Execute the Business Continuity Plan, when the plan is active.

d) Business Continuity Coordinators (BCCs)

The Governance and Compliance Divisional Heads within departments fulfil the role of BCCs for their departments. In the absence of a Governance & Compliance Division or Divisional Head, the role responsible for risk management activities within a department shall fulfil the business coordinator role.

The role responsible for risk management activities for the entity shall fulfil the business continuity coordinator role.

BCCs are responsible to develop, maintain, exercise and execute the BCPs as delegated by the respective HoDs.

BCCs shall:
- Regularly conduct Business Impact Analyses (BIA) on own systems, procedures and services, at least annually;
- Determine and propose appropriate actions to reduce Business Continuity risks.
- Design and operate systems with resilience and ease of recovery in mind;
- Develop BCPs, Procedures and checklists for identified systems and processes;
- Execute projects and activities to enhance resilience of systems, services and procedures;
- Regularly facilitate the exercise of BC activities; and
- Continuously improve BC documents and initiatives.

e) Incident Response Teams

Incident Response Teams, established in terms of the BCP of a department or municipal owned entity, are responsible for managing the resolution of an incident that may have resulted in the invocation of the BCP.

The Incident Response Team members will be appointed by the respective HOD in the case of a municipal owned entity.

5. Processes

5.1 The processes to be undertaken to develop appropriate business continuity solutions will involve:

- The identification of departmental processes;
- An evaluation of the criticality of these processes;
- An evaluation of their service delivery and financial impacts;
- Determination of critical delivery periods and times frames for these processes;
- Assessment of Inter-departmental dependencies;
- Assessment on the extent of reliance on third parties to carry out certain processes;
- Identification of the legislative/regulatory requirements associated with processes;
- A determination of the recovery time frames
- A determination of the human and other physical resources necessary to undertake a particular process;

-    Identification and evaluation of the root causes of risks that may have the potential for disruption of processes

5.2   The above processes shall be performed in line with the Business Continuity Management Framework & Methodology.

5.3   The outcome of the above processes will be various business continuity solutions, including:
-    Organisation-wide business continuity strategies for aspects such as:
    - Alternative recovery locations/sites,
    - Strike plans,
    - Crisis Communication
    - Coordination between Emergency Response, BCM and Disaster Risk Management to optimise overall municipal resilience
-    Business continuity plans for all urgent service-delivery critical processes,
-    Risk management response plans to proactively address the identified business disruption risks.

5.4   The success of the EMMs BCMS is reliant on:

5.4.1. Funding - Adequate provision shall be made to fund the implementation of the Business Continuity Programme within the EMM Departments.

5.4.2. Benchmarking - Benchmarking techniques and process shall be employed by the EMM BCM role players focusing on industry best practices, in order to achieve the stated BCM objectives.

5.4.3. Training and awareness - Training and awareness activities will be undertaken to ensure that:
    - Those tasked with various Business Continuity related responsibilities are empowered to fulfil those responsibilities; and
    - There is increased and enhanced awareness of BCM throughout the EMM.

6.   Systems and Tools

6.1 Document repository
BC role players need to be familiar, understand, and trained in the exercising of incident management documentation and BCPs. Relevant BCM documentation will be readily available to all employees on the intranet and hard copy. The EMM will make use of the Battle- box portfolio.

The Battle-box will contain concise incident management documentation during a disruption to be used as a first response in managing the evacuation process, ensuring effective communications that will support the entire incident process in a very efficient manner. The documentation will be supported by essential incident management and business continuity management documentation which can mean the difference between success and failure in responding effectively to a disruption.

Provision for the battle-box to be accessible at the identified command centre/s will be documented in the Strategy Report.

6.2 Maintenance and testing of BCPs

The developed BCM solution will be maintained continuously in a fully deployable capability in terms of a maintenance strategy which will be signed off by the ICT and Service Continuity Steering Committee. Exercising of system and process recovery will occur at least annually. Test results shall be documented in accordance to good practice guidelines.

Ongoing validation of BCM will be subjected to the scrutiny of external and internal auditors, to ensure that organizational maturity is continually improved.

Change Control procedures will be amended to incorporate BCM requirements.

6.3 Outsourcing

All companies deemed to be critical to the Group's supply chain will be encouraged to employ similar standards of BCM.

7. Assumptions

EMMs BCMS maturity will improve if the key performance indicators or BCM enablers, as detailed in section 3 to 6 of the policy, are noted and implemented.

Annexure A: Glossary of terms and abbreviations

The following terminologies (where applicable) are based on the ISO 22301 standard, the BCI's Good Practice Guidelines and the EMM Disaster Management Plan:

Term	Definition
Battle-Box	A container often literally a box or brief case in which information e.g. BCP is stored so as to be immediately available to those responding to a disruption.
Business Continuity	Capability of the organisation to continue delivery of products or services at acceptable predefined levels following disruptive incident.
Business Continuity Institute	The BCI is a Global Membership Institution for Business Continuity Professionals. The overall purpose is to promote the art and science of business continuity worldwide.
Business Continuity Management	Holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.
Business Continuity Management Lifecycle	The stages of activity that an organisation moves through and repeats with the overall aim of improving organisational resilience.
Business Continuity Management System	Ongoing management and governance process supported by top management and appropriately resourced to implement and maintain business continuity management.
Business Continuity Plan	Documented procedures that guide organisations to respond, recover, resume and restore to a predefined level of operation following disruption.
Business Impact Analysis	Process of analysing activities and the effect that a business disruption might have upon them.
Crisis	A situation with a high level of uncertainty that disrupts the core activities and/or credibility of an organisation and requires urgent action.

Term	Definition

Disaster	A progressive or sudden, widespread or localised, natural or human-caused occurrence which-
	
	a) Causes or threatens to cause-
	    I. Death, injury or disease;
	    II. Damage to property, infrastructure or the environment; or
	    III. Disruption of the life of a community; and
	b) Is of a magnitude that exceeds the ability of those affected by the disaster to cope with its effects using only their own resources.

Disruption	A disruption is a major disturbance, something that changes your plans or interrupts an event, activity or process.
Recovery Time Objective	Period of time following an incident within which: • Product or service must be resumed, or • Activity must be resumed, or • Resources must be recovered.
Resilience	Adaptive capacity of an organisation in a complex changing environment.
Risk	Effect of uncertainty on objectives.
Risk Assessment	Overall process of risk identification, risk analysis and risk evaluation.
Risk Management	Coordinated activities to direct and control an organisation with regard to risk.

The following abbreviations relate to this Policy.

Abbreviations	Term
BCI	Business Continuity Institute
BCM	Business Continuity Management
BCP	Business Continuity Plan
BIA	Business Impact Analysis
GPG	The GPG: 2014 is a document for anyone interested in Business Continuity (BC) and the good practices shared by practitioners from around the world in many different types of organizations. It contains the Business Continuity Management (BCM) Lifecycle and a description of the six 'Professional Practices' at a managerial and technical level used by BC practitioners worldwide to develop, manage, implement and validate their BCM programmes
HR	Human Resources
OHS	Operational, Health and Safety

Abbreviations	Term
ISO 22301: 2012	International Standards Organisation (ISO 22301:2012) specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise. The requirements specified in ISO 22301:2012 are generic and intended to be applicable to all organizations, or parts thereof, regardless of type, size and nature of the organization. The extent of application of these requirements depends on the organization's operating environment and complexity
IT	Information Technology
KPA	Key Performance Area
KPI	Key Performance Indicator
PAIA	Protection of Personal Information Act
PFMA	Public Financial Management Act
RTO	Recovery Time Objective