dcstm

Department:
Community Safety and Transport Management
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

NDP 2030

DEPARTMENT OF COMMUNITY SAFETY AND TRANSPORT MANAGEMENT

BUSINESS CONTINUITY MANAGEMENT POLICY
2025/2026

BCM Policy 2025/26

1. GLOSSARY OF TERMS

Abbreviation	Term	Description
BIA	Business Impact Analysis	The process by which the impact of a disaster on a business unit or function is assessed in terms of people, environmental, social, technological, legislative and economic impacts.
BCMS	Business Continuity Management System	A holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.
BCSC	Business Continuity Steering Committee	A tactical committee responsible for making recommendations to the Business Continuity Steering Committee regarding the BCM programme.
BCP	Business Continuity Planning	The process of developing advance arrangements and procedures that enable an organisation to respond to an event in such a manner that critical business functions continue with planned levels of interruption.
BRC	Business Recovery Coordinator	The Business Recovery Coordinator has overall accountability and responsibility for

		the coordination of the Business Continuity Recovery, the recovery strategy and overall monitoring of all BCM processes.
CIO	Chief information officer	An official within the department appointed responsible for the **information** technology and computer systems that support departmental goals.
ERM	Enterprise risk management	Is an application of risk management processes within the entire department, instead of only to certain activities or programmes
HoD	Head of the Department	Means an officials appointed in terms of section 38 of the PFMA as the accounting officer for the department
IT DRP	Information Technology Disaster Recovery Plan	The document that defines the resources, actions, tasks and data required to manage the business recovery process in the event of a business disruption. The plan is designed to assist in restoring the business process within the stated disaster recovery goals.
RA	Risk Assessment	A formal process of risk identification, risk analysis and risk evaluation.
ORM	Operational risk management	The identification and management of risks at business level to ensure integration into the day-to-day operations of the department
CG	Corporate Governance	The Audit Commission has defined corporate Governance as "The systems and processes

		by which department led, direct and control their functions, in order to achieve their objectives, and by which they relate to their partners and the wider community". To achieve these objectives, the Department need to be capable of ensuring the continuity of their critical infrastructure, core services, systems and essential business processes.

2. POLICY STATEMENT

The overall objective of the Business Continuity Management System is to fully and reliably ensure the continued efficient operation of the Department in a manner, which maintains adequate standards of confidentiality, data integrity and availability.

Management of the Department is committed to complying with the requirements and maintaining the effectiveness and continual improvement of the Business Continuity Management System, which support the Department's business strategy. It will also ensure adequate resources allocation and focus its energy on management of this critical endeavour.

Guidance on procedures to be followed in the event of a disruptive incident can be found in Business Continuity Management Plans, which are accessible to all personnel.

3. DEFINITION

Business Continuity Management System (BCMS) refers to a holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities. (Extract from BS25999 Part 1)

Business Continuity (BC) refers to a state of continued, uninterrupted operation of the department in all contexts. It focuses on the resiliency of people, property, processes, platforms and providers as well as the availability and integrity of information.

A Business Continuity Plan is invoked after a disruptive event has occurred – it is not about preventing a disruptive event from occurring. This disruptive event is normally a very low probability but very high consequence event.

Business Continuity Planning also presents the opportunity for the Department to review their business approach, examine processes, improve procedures and practices and thereby improve the organisation's resilience to loss of, or interruption to their services and systems.

Business Continuity Planning forms an integral part of Corporate Governance for the Department.

4. PURPOSE

The overall objective of this policy is to provide guidance to management for an orderly and timely recovery from a disaster or disruptive incident in order to:

a. Protect the operations of the department, licensees, stakeholders and staff by minimising the impact of serious interruption to the department through the effective implementation and maintenance of BCM arrangements.

b. Recover the critical operations in a planned and controlled manner to meet the requirements of the department, law, regulations or other factors.

c. Ensure that business continuity is an essential part of business planning and future development.

5. LEGISLATIVE FRAMEWORK

a. Public Finance Management Act, 1999 (Act No. 1 of 1999), as amended including the Treasury regulations, 2005, as amended

b. The Disaster Management Act (Act No. 57 of 2002) defines a disaster as a progressive or sudden, widespread or localised, natural or human-caused occurrence which:

Causes or threatens to cause:

    i.   Death, injury or disease

    ii.   Damage to property, infrastructure or the environment

    iii.   Disruption of the life of the community.

Other Acts relevant to the BCMS include:

    c. Promotion of Access to Information Act, 2000 (Act No 2 of 2000)

    d. Electronic Communications and Transactions Act (ECTA), 2002 (Act No. 25 of 2002)

    e. Minimum Information Security Standards

    f. Occupational Health and Safety Act

    g. Good governance benchmarks like;

    h. BCI good practice guideline and ISO 22301

6. APPLICATION AND THE SCOPE OF THE POLICY

Business Continuity Management policy is a core component of good corporate governance; it should be applied across the entire Department, by all employees at Head office, District offices, Stations, Registering Authorities, Government garages, DLTC and VTS's, Operating Licenses and Permit offices. Corporate Services processes or functions like Human Resource management, Supply Chain Management process, Payment of Suppliers equally plays a critical role in business continuity process. The policy is aimed at guiding continued service delivery by ensuring that the Department's mandate is realised, i.e." *To promote community and road safety through community mobilisation, positively influencing road user behaviour through safety awareness and traffic law enforcement; oversight of the police and to coordinate public transport services.*"

Following are examples of instances where Business Continuity Management interventions should apply:

    a. severe effects on human lives and well-being, directly or indirectly;

    b. severe outage to the critical processes;

    c. severe damage to the critical assets of Department

 d. severe damage, or loss, to Department 's data and information;

 e. severe damage to Department 's IT infrastructure and services;

 f. Severe damage, or impact, to Department s reputation, brand, and public perception.

7. BENEFITS OF THE BCM

The policy provides a clear commitment to business continuity management. Effective business continuity will enable the employees of the Department and stakeholders to:

 a. Continue to provide critical services to the public even during the times of disruptions

 b. Make the best use of personnel and other resources at times when both may be scarce.

 c. Reduce the period of disruption to the Department and the public we serve

 d. Resume the normal business more efficiently and effectively after the period of disruption.

 e. Improve the resilience of the Department 's infrastructure to reduce the likelihood of disruption.

 f. Reduce the operational and functional impact of any disruption.

8. KEY PLANS IN THE BUSINESS CONTINUITY MANAGEMENT SYSTEM

8.1. BCM METHODOLOGY/FRAMEWORK

The framework aims to assist the user put the theory of Business Continuity Management into practice by guiding the Department through the steps needed to implement Business Continuity Management System.

8.2. CRISIS MANAGEMENT PLAN

The plan intends to guide proper communication relating to the incident; i.e.

 a. Communication before, during and after the event/incident including targeted communication for employees, clients, regulatory bodies, and all those affected by the event.

 b. It also pertains to informing the media, stakeholders, emergency services, etc, about the disaster.

c. It is also intended to guide the Crisis Management Team ("CMT") in assessing the incident (e.g. how severe is the incident).

8.3 EVACUATION PLAN

The purpose of a plan is to facilitate and organize employer and employee actions during workplace emergencies. It is intended to guide the evacuation of employees from the danger zone; also ensures that clients/ employees are calm and are evacuated in and an orderly and safe manner.

8.4 IT DISASTER RECOVERY PLAN

The objective of the IT disaster recovery plan is to assist the Department in recovering the IT services and infrastructure as directed by the plan.

8.5. BUSINESS CONTINUITY AND RECOVERY PLAN

Continuity and recovery plans are intended to direct processes towards restoring full operational capability and returning to business-as-usual after the crisis is over.

9. ROLES AND RESPONSIBILITIES

9.1 Accounting officer

a. Ensure that the BC Plan adequately reflects the Department's BC capability.
b. Provide leadership, commitment and resources as part of governance.
c. The Accounting Officer who is also the business recovery leader has overall responsibility and accountability for the effective management of the incident response and will lead the Business Recovery Team.
d. He has the responsibility to declare the start/end of disasters and invoke/end the relevant actions and plans with the assistance of Management/Steering committee.

9.2 Management

Management is responsible for ensuring that policies and objectives are established for the business continuity management system and are compatible with the strategic direction of the Department, this will be achieved by:-

a. Identifying threats (hazards) to core business function continuity and the processes, systems, information, people, assets, outsource partners and other resources that support or rely on them.

b. Systematically analyses likelihood and consequence of disruption and rate using the consequence ratings in the risk management strategy;

c. Evaluate which disruption-related risks require treatment; and

d. Identify treatments commensurate with BC objectives and in accordance with the Department's risk appetite.

e. Ensuring the integration of the business continuity management system requirements into the organization's business processes

f. Ensuring that the resources needed for the business continuity management system are available

g. Communicating the importance of effective business continuity management and conforming to the BCMS requirements

h. Ensuring that the BCMS achieves its intended outcome(s)

i. Directing and supporting officials to contribute to the effectiveness of the BCMS

j. Promoting continual improvement, and

k. Supporting other relevant management roles to demonstrate their leadership and commitment as it applies to their areas of responsibility.

9.3 Business Continuity Management teams

The Department and the BCM teams shall conduct self-assessments bi-annually (sixth monthly) to ensure that the Continuity Plans are up-to-date.

9.3.1 BCM Steering Committee

a. Oversee, manage and advise the BC programme making recommendations and reporting to top management by;

b. Communicate the implications of departmental changes that may impact on the BC programme.

c. BCM Steering Committee meetings should be held at least quarterly to review BCM issues and progress.

9.3.2 *BCM Technical Committee*

a. Making recommendations to the Business Continuity Steering Committee regarding the BCM programme and taking forward actions on its behalf;

b. Assisting with the review and development of the Business Continuity Management programme and support continuous improvement of the Programme including;

    i. Updating this Business Continuity Policy as appropriate

    ii. Receiving status reports on Business Continuity and identifying any actions

    iii. Identifying cross cutting issues and coordinating planning including prioritizing actions from BCSC, incidents, exercises etc.

c. Supporting the Business Continuity PR actioners in raising the profile of Business Continuity by ensuring that the programmes within the departments are engaged.

d. Supporting the exercising of plans to ensure that they remain up to date and fit for purpose.

e. Ensuring that there is a consistent approach to Business Continuity across the Department, in accordance with the BCM Programme

f. Leading on the development of the Department's Incident Management planning arrangements

g. Including the review and development of the Major Incident Plan, reporting on the arrangements in place and ensuring the plan is exercised on an annual basis (unless a major incident occurs that has "tested" arrangements in the plan).

9.4 Risk Management Unit

a. The Risk Management Unit must ensure steps are taken to periodically conduct risk assessments and business impact analysis

b. Review the BCMS policies, procedures and plans to identify potential non-conformities and their causes to reduce or eliminate the chances for BCM failures.

c. All such action taken shall be documented appropriately.

d. It shall also ensure that opportunities presented by implementation and operation of BCMS are taken advantage of and non-conformities identified along the process are eliminated to avoid recurrence.

e. Develop and deliver an effective BC Programme this includes facilitation and coordination of plans throughout the organization.

9.5 Officials

It is important that everyone in the Department is aware of the BCM Programme. Staff should be made aware of any arrangements in their directorate's plan that may affect them e.g. how they will be contacted / notified of an incident, where they should report to if they are not able to access their usual place of work. Staff or personnel within the Department should also amongst other be able to;

a. Recognizes an incident or crises,

b. Alert incident /crises responders

c. Escalate action to the incident or crises management team

d. Respond appropriately to specific threat

e. Respond appropriately when evacuated from the site

f. Understand relevant plans and associated roles and responsibilities

9.6 Internal Audit

The Department's Internal Audit function shall, as part of their annual planning exercise, include BCMS activities and plans for all applicable Directorates / functional units or for any ad-hoc reviews.

10. BCM TRAINING AND AWARENESS

Embedding the business continuity takes inculcating the culture of risk management holistically. All officials, including temporary staff, shall be trained and/or made aware of relevant BCM information at least once a year so that they are familiar with the BCMS, policy, communication and recovery plans and procedures, and are confident in their roles during an incident. Some avenues for training include:

a. DMC and team meetings/planning days;

b. Employee orientation;

c. Risk management training or specific BC training;

d. Risk chats circulated through email

e. Emergency evacuation testing and other testing procedures.

11. BCM MAINTENANCE

The BCMS shall be continuously monitored to ensure that changes in the way business functions are incorporated and changes in the supporting infrastructure are reflected in the BCMS Strategy, Procedures and Plans. Improvements identified because of testing and training shall be included in the BCP. All changes shall be assessed as part of change management.

12. FAILURE TO COMPLY WITH THIS POLICY

a. Safety of employees and continuity of operations during an incident is the responsibility of everyone affiliated with the Department or directly accessing the Department's premises, systems, data in any form and information entrusted to the Department by other third parties.

b. The BCMS related policy statements described above define the basic minimum level of requirements for safety, availability and continuity of the Department's resources and services.

c. Non-compliance with the required measures and behaviors outlined in this policy could pose significant business and legal risks to the Department and may create a potential for legal actions that could significantly affect the Department's operations and damage its assets and reputation.

d. Therefore, compliance with all the Department's BCMS-related policies is a mandatory conditions of employment for all staff, as well as any third parties (such as outsourcing providers, contractors, alliance partners, clients, etc.).

e. No one is permitted to bypass the BCMS related Policy statements provided by the Department for any reason. Failure to comply with this policy will be reported and disciplinary action may be taken against any person violating its provision.

13. EXCEPTIONS, MIGRATIONS AND TIMEFRAMES.

a. All Department personnel and systems must comply with the provisions in this policy from the date of its approval.

b. Where a longer transition is required to achieve compliance, a documented justification must be submitted with proposed timelines as an exception to the Department's Accounting Officer for the approval.

c. Any exceptions to this Policy must be clearly documented and submitted to the Accounting Officer for evaluation and approval. Only exceptions, which have been approved, are valid.

d. All exceptions to this Policy will be fully motivated and documented by those seeking the exception, and agreed to by the relevant affected parties. All exceptions will be reviewed at least annually by the relevant Individual/s tasked with risk management around the particular area/s affected by the exception.

14. REVIEW OF THE POLICY

This policy shall be reviewed annually or as and when the need arises. This policy shall take effect immediately after the Accounting Officer has approved.

15. RECOMMENDATION AND APPROVAL

DISCUSSED AND ADOPTED DURING	DATE
DEPARTMENTAL MANAGEMENT COMMITTEE (RMC)	25/.03/2025
DEPARTMENTAL RISK MANAGEMENT COMMITTEE (DMC)	2.6/.03/2025

RECOMMENDED

CHAIRPERSON RMC
Mr. A KYEREH
DATE: 27/03/2025

APPROVED

DR. HANS KEKANA
HEAD OF DEPARTMENT
DATE: 31/03/2025