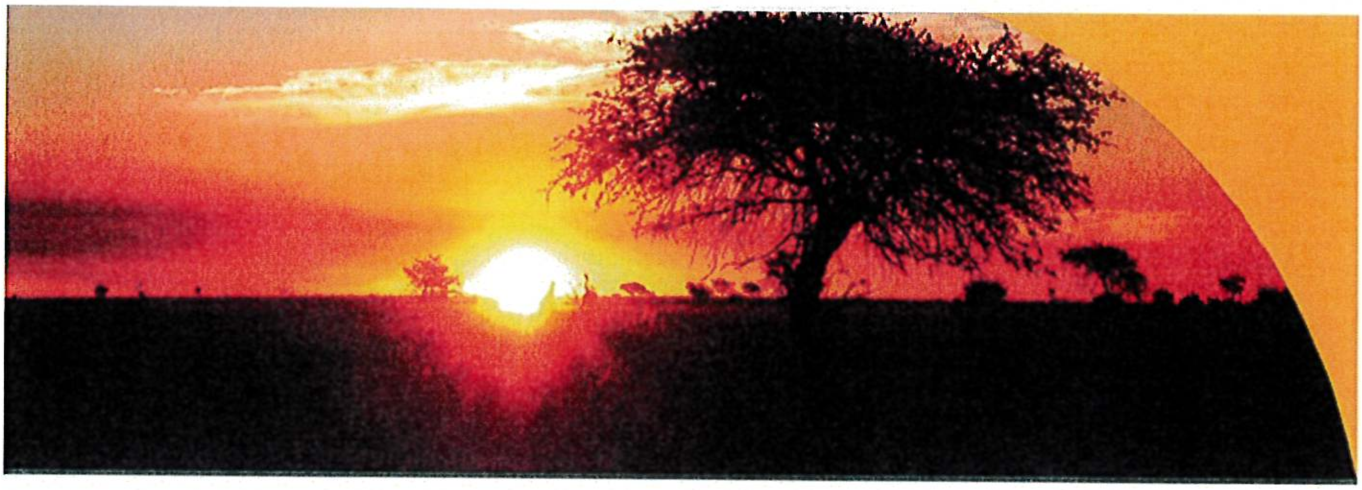

DCSR POLICY: BUSINESS CONTINUITY MANAGEMENT POLICY

DOCUMENT INFORMATION AND LOG

File Name	**Business Continuity Management Policy**
Original Author	**Department of Culture, Sport and Recreation**
Review Date	**2028 / 2029**

1. PREAMBLE

The Department of Culture, Sport and Recreation (DCSR) is mandated to promote, develop and preserve culture, heritage, libraries, archives, sport and recreation services for the benefit of the citizens of the Province. The Department recognises that disruptive incidents may adversely affect its ability to deliver essential services, achieve strategic objectives and fulfil statutory obligations.

Business Continuity Management (BCM) is a critical component of sound governance, risk management and organisational resilience. BCM ensures that the Department is able to continue delivering critical services during and after disruptive events through proactive planning, preparedness, response and recovery measures.

This policy establishes the principles, governance structures, responsibilities and requirements for implementing an effective BCM programme throughout the Department.

2. PURPOSE OF THE POLICY

The purpose of this policy is to:

- Establish a structured Business Continuity Management framework within the Department.
- Enhance organisational resilience against disruptions.
- Ensure continuity of critical departmental services and functions.
- Minimise operational, financial, legal, reputational and strategic impacts arising from disruptions.
- Ensure compliance with applicable legislative and regulatory requirements.
- Protect employees, assets, information, systems and stakeholders.
- Provide guidance for business continuity planning, testing, maintenance and continuous improvement.
- Facilitate timely recovery of critical services following disruptions.

3. LEGISLATIVE AND REGULATORY FRAMEWORK

This policy derives authority from:

- Constitution of the Republic of South Africa, 1996.
- Public Finance Management Act, 1999 (Act 1 of 1999).
- Treasury Regulations.
- National Treasury Risk Management Framework.
- Public Service Act, 1994.
- Public Service Regulations.
- Occupational Health and Safety Act, 1993.
- Disaster Management Act, 2002.
- Protection of Personal Information Act, 2013.
- National Archives and Records Service Act, 1996.
- Electronic Communications and Transactions Act, 2002.
- King IV Report on Corporate Governance.
- DPSA Business Continuity Management Guidelines.
- National Cybersecurity Policy Framework.
- Provincial Risk Management Frameworks and Directives.

4. OBJECTIVES OF BUSINESS CONTINUITY MANAGEMENT

Business Continuity Management is intended to ensure that the Department can continue to deliver its mandate during and after disruptive incidents. The BCM Programme supports organisational resilience by identifying critical functions, protecting key resources and establishing recovery mechanisms that minimise service interruptions. Through effective planning and preparedness, the Department seeks to safeguard service delivery, public confidence and institutional sustainability.

The objectives of BCM are to:

4.1 Ensure Service Delivery Continuity

The Department delivers essential public services relating to culture, libraries, archives, sport and recreation. Any prolonged interruption to these services may negatively affect communities, stakeholders and strategic objectives. BCM therefore seeks to ensure that critical services remain operational during adverse events.

- Maintain uninterrupted delivery of critical services relating to:
    - Cultural Affairs
    - Libraries
    - Archives and Records Management
    - Sport Development
    - Recreation Programmes
    - Heritage Preservation
    - Administrative Support Services

4.2 Protect Stakeholders

The Department has a responsibility to protect the wellbeing of employees, service beneficiaries and stakeholders who rely on its services. BCM measures must therefore include provisions that ensure the safety and protection of all affected parties during disruptions.

- Safeguard:
    - Employees
    - Service beneficiaries
    - Communities
    - Government partners
    - Service providers
    - Public resources

4.3 Enhance Organisational Resilience

Resilience refers to the Department's ability to anticipate, prepare for, respond to and recover from disruptive incidents. BCM contributes to resilience by establishing procedures and controls that strengthen organisational adaptability and recovery capacity.

- Develop the Department's capacity to:
    - Anticipate disruptions
    - Respond effectively to incidents
    - Recover operations rapidly

    - Adapt to changing circumstances

4.4 Reduce Operational Disruptions

Disruptions often result in financial losses, service delays, reputational damage and stakeholder dissatisfaction. Effective BCM seeks to minimise these impacts through proactive planning and coordinated response mechanisms.

- Minimise:
    - Downtime
    - Service interruptions
    - Financial losses
    - Data losses
    - Reputational damage

5. SCOPE OF APPLICATION

This policy establishes the BCM requirements applicable across the Department. BCM is not limited to information technology or emergency response activities but applies to all business operations, facilities, employees, systems and service providers that support the Department's mandate. Every programme and business unit has a responsibility to contribute towards organisational continuity and resilience.

This policy applies to:

- All DCSR programmes
- All directorates and units
- All employees
- Contract workers
- Interns
- Service providers
- Consultants performing functions on behalf of the Department
- All departmental facilities and offices
- Information systems and technology infrastructure
- Libraries, archives, museums and cultural facilities under the Department's control
- Sporting and recreational facilities managed by the Department

6. POLICY PRINCIPLES

The effectiveness of Business Continuity Management depends on adherence to sound governance principles. These principles guide the implementation, maintenance and continuous improvement of BCM across the Department and ensure alignment with risk management and governance practices.

The Department shall implement BCM in accordance with the following principles:

6.1 Governance

Business Continuity Management shall be embedded within the Department's governance structures to ensure accountability, oversight and strategic alignment. BCM must form part of the broader governance, risk and compliance environment.

- BCM shall be integrated into the Department's governance, risk management and strategic planning processes.

6.2 Accountability

Successful BCM implementation requires clear ownership and accountability. Management at all levels must take responsibility for ensuring continuity arrangements within their areas of control.

- Management shall be accountable for continuity planning within their areas of responsibility.

6.3 Risk-Based Approach

BCM activities shall be informed by risk assessments and evidence-based decision-making processes. Resources shall be prioritised according to the significance of identified risks and potential impacts.

- Business continuity planning shall be informed by risk assessments and Business Impact Analyses.

6.4 Continuous Improvement

The BCM programme shall remain dynamic and responsive to changing risks, technologies and organisational needs. Regular reviews and testing will ensure ongoing effectiveness.

- BCM shall be reviewed, tested and improved continuously.

6.5 Compliance

All BCM activities shall be undertaken within the framework of applicable legislation, regulations and recognised best practices.

- BCM activities shall comply with applicable legislation, regulations and standards.

6.6 Organisational Resilience

The Department shall cultivate a culture of preparedness and resilience that empowers employees to respond effectively to disruptions.

- The Department shall promote a culture of preparedness and resilience.

7. BCM GOVERNANCE STRUCTURE

Effective BCM requires clearly defined governance structures that provide leadership, oversight and accountability. The governance framework establishes roles and responsibilities for officials responsible for planning, implementing, monitoring and improving BCM across the Department.

The following governance structures shall support BCM implementation:

7.1 Accounting Officer

As the head of the Department, the Accounting Officer bears ultimate responsibility for ensuring that BCM arrangements are established, maintained and adequately resourced. The Accounting Officer provides strategic direction and oversight of the BCM programme.

The Accounting Officer shall:

- Provide BCM leadership.
- Approve BCM policies and plans.
- Ensure adequate resources are allocated.
- Monitor BCM implementation.
- Report significant continuity risks.

7.2 Executive Management Committee

The Executive Management Committee provides strategic oversight and ensures that BCM remains aligned to departmental objectives and priorities.

The Committee shall:

- Oversee BCM implementation.
- Review BCM performance reports.
- Monitor strategic continuity risks.
- Approve continuity improvement initiatives.

7.3 Ethics and Risk Management Committee

The Risk Management Committee provides independent oversight of BCM and ensures that continuity risks are appropriately managed.

The Committee shall:

- Monitor BCM effectiveness.
- Review continuity risks.
- Recommend improvements.
- Provide assurance regarding BCM implementation.

8. BUSINESS CONTINUITY MANAGEMENT FRAMEWORK

The BCM Framework provides a systematic approach to identifying threats, assessing impacts, implementing continuity strategies and maintaining recovery capabilities. The framework ensures that BCM activities are integrated into risk management and operational planning processes.

The BCM Framework shall comprise the following components:

8.1 Risk Assessment

Risk assessment forms the foundation of BCM. It enables the Department to identify threats that may disrupt service delivery and evaluate their potential impact on operations, assets, stakeholders and strategic objectives.

The Department shall identify and assess threats including:

Natural Disasters

Natural events may cause significant operational disruptions, facility damage and service interruptions.

- Floods
- Storms
- Fires
- Droughts

Technological Failures

Technology failures can affect critical business systems, communications and information management capabilities.

- System outages
- Network failures
- Data corruption
- Cyber-attacks

Human-Caused Incidents

Human actions, whether intentional or accidental, may disrupt operations and compromise organisational resources.

- Sabotage
- Fraud
- Theft
- Labour unrest

Infrastructure Failures

The Department's operations depend on reliable infrastructure and utilities. Interruptions may severely affect service delivery.

- Electricity outages
- Water interruptions
- Telecommunications failures

Health Emergencies

Health-related incidents can affect workforce availability and operational capacity.

- Pandemics
- Epidemics
- Occupational health incidents

9. BUSINESS CONTINUITY PLANS

Business Continuity Plans (BCPs) are the cornerstone of the Department's Business Continuity Management Programme. A Business Continuity Plan is a documented set of procedures, resources, responsibilities and recovery actions designed to enable the Department to continue delivering critical services during and after a disruption. The purpose of a BCP is not only to restore operations following an incident but also to ensure that critical functions can continue at an acceptable level while recovery activities are underway.

The Department's Business Continuity Plans shall address the following components:

9.1 Identification of Critical Business Functions

The first step in continuity planning is the identification of critical business functions and services that are essential to the Department's ability to fulfil its legislative mandate and strategic objectives. These functions must be prioritised for recovery based on their importance to service delivery and the potential consequences of prolonged disruption.

The identification process shall be informed by Business Impact Analyses (BIAs), risk assessments and management consultations.

9.2 Recovery Time Objectives (RTOs)

Recovery Time Objectives (RTOs) represent the maximum acceptable period within which a critical service, process or system must be restored following a disruption.

The Department shall establish realistic and achievable recovery timeframes for all critical activities.

9.3 Recovery Point Objectives (RPOs)

Recovery Point Objectives define the maximum amount of data loss that the Department is willing to tolerate following a disruption.

The Department shall establish RPOs for all critical information systems and electronic records.

Factors to be considered include:

- Availability of backup systems.
- Frequency of data updates.
- Importance of information.
- Regulatory requirements.
- Financial implications of data loss.

9.4 Continuity Strategies

The Department shall develop continuity strategies that enable critical services to continue during disruptions. These strategies shall be designed to reduce operational downtime and support the timely restoration of normal operations.

Continuity strategies may include:

- **Alternative Work Arrangements**

Where facilities become inaccessible or unsafe, alternative work arrangements may be activated.

These may include:

- Remote working arrangements.
- Hybrid working models.
- Temporary relocation of personnel.
- Shared workspaces.
- Rotational staffing schedules.

- **Alternate Service Delivery Methods**

Where traditional service delivery methods are disrupted, alternative methods shall be considered.

These may include:

- Virtual service delivery platforms.
- Online stakeholder engagement.
- Mobile service units.
- Digital communication channels.
- Remote programme implementation.

- **Resource Redundancy**

The Department shall establish backup resources to support continuity.

These may include:

- Backup equipment.
- Alternative communication tools.
- Emergency procurement arrangements.
- Additional service providers.
- Standby technical support.

9.5 Business Continuity Plan Documentation

All continuity arrangements shall be formally documented and maintained in a standardised format to ensure consistency across the Department.

Each Business Continuity Plan shall include:

Governance Information

- Name of business unit.
- Plan owner.
- Approval authority.
- Date of approval.
- Date of review.

Purpose and Scope

- Description of the business unit.
- Scope of continuity arrangements.
- Critical services covered.

Critical Processes

- List of essential activities.
- Priority rankings.
- Recovery time requirements.

Dependencies

- Human resource requirements.
- Technology requirements.
- Facilities and infrastructure requirements.
- Supplier dependencies.
- Information requirements.

Recovery Procedures

- Immediate response actions.
- Recovery activities.
- Escalation processes.
- Resource mobilisation procedures.

9.6 Emergency Contact Lists

Effective communication is essential during a disruptive event. The Department shall maintain updated contact information to support timely communication and decision-making.

Business Continuity Plans shall include:

Internal Contacts

- Head of Department.
- Chief Financial Officer.
- Programme Managers.
- ICT personnel.
- Risk Management officials.
- Security personnel.
- Communications officials.

External Contacts

- Emergency services.
- Provincial Disaster Management Centre.
- Provincial Treasury.
- Key service providers.
- Telecommunications providers.
- ICT support providers.
- Security companies.

9.7 Communication and Stakeholder Management

During a disruption, effective communication is critical to maintaining stakeholder confidence and ensuring coordinated response efforts. The Department shall establish communication protocols that provide clear guidance regarding information sharing and stakeholder engagement.

Communication plans shall address:

Internal Communication

- Employee notifications.
- Management briefings.
- Emergency instructions.
- Recovery progress updates.

External Communication

- Public announcements.
- Stakeholder notifications.
- Media responses.
- Government reporting requirements.

Only authorised spokespersons shall communicate externally on behalf of the Department.

9.8 Resource Requirements

The Department shall identify and secure the resources necessary to support continuity and recovery activities.

Resource requirements may include:

Human Resources

- Critical personnel.
- Alternate personnel.
- Emergency response teams.
- Technical specialists.

Technology Resources

- Laptops and computers.
- Servers and storage systems.
- Network connectivity.
- Communication devices.

Facilities

- Alternate office accommodation.
- Meeting facilities.
- Storage facilities.
- Emergency operations centres.

Financial Resources

- Emergency funding provisions.
- Procurement arrangements.
- Contingency budgets.

9.9 Supplier and Third-Party Continuity

The Department relies on numerous external service providers to support service delivery. Disruptions affecting these providers may have significant operational consequences.

The Department shall assess the continuity capabilities of critical suppliers and service providers.

Critical suppliers may include:

- ICT service providers.
- Telecommunications providers.
- Security service providers.
- Facility management contractors.
- Utility providers.
- Cloud service providers.

Service Level Agreements (SLAs) shall, where possible, include:

- Business continuity requirements.
- Disaster recovery provisions.

- Service restoration commitments.
- Incident reporting obligations.

9.10 Testing and Exercising

Business continuity plans are only effective if they are regularly tested and validated. Testing enables the Department to evaluate the effectiveness of continuity arrangements, identify weaknesses and ensure that employees understand their roles and responsibilities during disruptions.

The Department shall establish a structured testing and exercising programme to assess the readiness and effectiveness of BCM arrangements.

10. INCIDENT RESPONSE AND CRISIS MANAGEMENT

Despite proactive risk management and continuity planning, disruptive incidents may still occur. The Department must therefore establish formal incident response and crisis management arrangements to ensure a coordinated, effective and timely response to emergencies. Incident response focuses on immediate actions required to contain and manage an event, while crisis management provides strategic leadership and oversight during major disruptions.

The objective of incident response and crisis management is to:

- Protect the health, safety and welfare of employees, stakeholders and service beneficiaries.
- Minimise disruption to critical departmental services.
- Preserve departmental assets, information and infrastructure.
- Ensure effective communication during emergencies.
- Facilitate the rapid restoration of normal operations.

The Department shall establish the following crisis management arrangements:

Crisis Management Team (CMT)

The Department shall establish a Crisis Management Team responsible for coordinating the overall response to major incidents.

The Crisis Management Team shall:

- Assess the nature and severity of incidents.
- Determine escalation requirements.
- Coordinate emergency response activities.
- Allocate resources required for response and recovery.
- Provide strategic direction during crises.
- Monitor recovery activities.
- Ensure effective stakeholder communication.

Incident Escalation

The Department shall establish formal escalation procedures to ensure that incidents are reported and managed at the appropriate level.

Escalation procedures shall include:

- Incident classification criteria.
- Reporting channels.
- Notification requirements.
- Activation thresholds for continuity plans.
- Crisis management activation procedures.

Emergency Response

Emergency response activities shall focus on protecting people and stabilising the situation.

Emergency response measures may include:

- Evacuation procedures.
- Emergency medical assistance.
- Emergency communications.
- Security interventions.
- Incident containment measures.

11. INFORMATION AND COMMUNICATION TECHNOLOGY CONTINUITY

Information and Communication Technology (ICT) systems are critical enablers of departmental operations and service delivery. Disruptions affecting ICT infrastructure can significantly impact the Department's ability to perform essential functions. ICT continuity planning is therefore a key component of the BCM Programme.

The Department shall implement ICT continuity measures to ensure that critical systems, applications, networks and data can be recovered within acceptable timeframes following a disruption.

The ICT continuity programme shall include:

Data Backup Management

The Department shall ensure that critical information is protected through secure and reliable backup arrangements.

This shall include:

- Daily backups of critical systems and data.
- Off-site storage of backup media.
- Cloud-based backup solutions where appropriate.
- Regular verification of backup integrity.

- Periodic backup restoration testing.

Disaster Recovery Planning

Disaster recovery planning shall focus on the restoration of ICT services following major incidents.

Disaster recovery plans shall include:

- Recovery procedures for critical systems.
- Recovery priorities and timelines.
- Roles and responsibilities.
- Recovery resource requirements.
- System restoration procedures.
- Recovery testing arrangements.

Cyber Resilience

Cybersecurity incidents represent a growing threat to public sector operations and service delivery. The Department shall implement measures to reduce cyber-related risks and improve resilience.

These measures shall include:

- Cybersecurity awareness training.
- Endpoint protection solutions.
- Access control measures.
- Vulnerability assessments.
- Incident response procedures.
- Network security monitoring.

Critical Systems Recovery

The Department shall identify and prioritise critical systems that support service delivery and governance functions.

Priority systems may include:

- Financial management systems.
- Human resource systems.
- Supply chain management systems.
- Records management systems.
- Library management systems.
- Archive management systems.
- Risk management systems.
- Performance information systems.
- Electronic document management systems.

11. TRAINING AND AWARENESS

The success of BCM depends on the awareness, preparedness and competence of employees. Regular training and awareness programmes ensure that officials understand continuity arrangements and can effectively perform their roles during disruptions.

The Department shall implement BCM awareness and training programmes to ensure:

- Employee awareness
- Understanding of BCM responsibilities
- Preparedness for disruptions
- Effective incident response

Training shall include:

- Induction training
- BCM awareness sessions
- Emergency preparedness training
- Simulation exercises
- Crisis management training

12. MONITORING, EVALUATION AND REPORTING

Continuous monitoring and evaluation are essential to ensure that the BCM Programme remains effective, relevant and aligned with organisational objectives. Monitoring activities provide management with assurance regarding the Department's level of preparedness and resilience.

The Risk Management Unit shall coordinate monitoring and reporting activities across the Department.

Monitoring activities shall include:

BCM Compliance Monitoring

The Department shall monitor compliance with BCM requirements and approved continuity plans.

Monitoring shall assess:

- Availability of continuity plans.
- Currency of BCM documentation.
- Completion of BIAs.
- Implementation of corrective actions.
- Training and awareness levels.

BCM Performance Monitoring

The effectiveness of BCM shall be assessed through measurable performance indicators.

Performance indicators may include:

- Percentage of business units with approved BCPs.
- Percentage of annual testing completed.
- Number of critical systems tested.
- Recovery time achievement rates.
- BCM training participation rates.

Incident Monitoring

The Department shall maintain records of disruptions and incidents affecting operations.

Incident monitoring shall evaluate:

- Root causes.
- Frequency of incidents.
- Impact severity.
- Recovery effectiveness.
- Emerging trends.

Reporting

Regular reports shall be submitted to relevant governance structures.

Reports shall be presented to:

- Executive Management Committee.
- Risk Management Committee.
- Audit Committee.
- Head of Department.

Reports may include:

- BCM maturity assessments.
- Testing results.
- Significant incidents.
- Corrective action status.
- Emerging continuity risks.

13. ROLES AND RESPONSIBILITIES

The successful implementation of BCM requires clear accountability across all levels of the Department. Every employee has a role to play in ensuring organisational resilience and continuity of service delivery.

The key roles and responsibilities are outlined below:

Head of Department

The Head of Department shall:

- Provide strategic leadership for BCM.
- Approve BCM policies and plans.
- Ensure adequate resources are available.
- Promote a culture of resilience.
- Monitor BCM implementation.

Chief Financial Officer

The Chief Financial Officer shall:

- Support BCM implementation through resource allocation.
- Ensure financial continuity arrangements are maintained.
- Monitor BCM-related expenditure.

Risk Management Unit

The Risk Management Unit shall:

- Coordinate the BCM Programme.
- Facilitate BIAs and risk assessments.
- Monitor BCM implementation.
- Provide BCM reports.
- Facilitate awareness and training.

Programme Managers

Programme Managers shall:

- Identify critical functions.
- Develop and maintain BCPs.
- Participate in testing exercises.
- Monitor continuity risks.
- Implement improvement actions.

Employees

Employees shall:

- Comply with BCM requirements.
- Participate in BCM training.
- Report incidents promptly.
- Support recovery activities when required.

14. POLICY REVIEW

This policy shall remain a living document and shall be reviewed at least once every three (3) years or when there are legislative changes, organisational restructuring, audit findings, emerging risks and lessons learned from incidents.

15. POLICY APPROVAL AND EFFECTIVE DATE

This policy becomes effective on the date of approval by the Head of Department and shall remain in force until amended, replaced or withdrawn.

The Department commits itself to implementing this Business Continuity Management Policy as part of its broader governance, risk management, compliance and organisational resilience framework to ensure the uninterrupted delivery of cultural, heritage, library, archive, sport and recreation services to the citizens of the Province.

MR EM MAHLANGU

HEAD: CULTURE, SPORT AND RECREATION

DATE 30 / 06 **/2026**