co-operative governance & traditional affairs
MPUMALANGA PROVINCE
REPUBLIC OF SOUTH AFRICA

BUSINESS CONTINUITY PLAN

2017/18

Business continuity Plan Policy 2017/18
TABLE OF CONTENTS

1. PREAMBLE ................................................................. 1
2. REGULATORY FRAMEWORK ......................................... 1
3. DEFINITIONS .............................................................. 1
4. OVERVIEW ................................................................. 2
5. OBJECTIVES OF THE BUSINESS CONTINUITY PLAN ............ 3
6. CURRENT ENVIRONMENT ................................................ 3
7. RISK AND THREAT ANALYSIS ........................................ 4
8. RISK ASSESSMENTS AND INFORMATION GATHERING ............. 5
9. ANALYSIS OF RESPONSIVENESS/CONTINUITY OF DEPARTMENT OF COOPERATIVE GOVERNANCE AND TRADITIONAL AFFAIRS ......... 6
10. TIMING AND MAINTENANCE OF THE BCP ......................... 7
11. CONCLUSION ............................................................ 7
12. APPROVAL .............................................................. 8
13. REVIEW OF POLICY ................................................... 8
14. CONTRAVENTIONS ..................................................... 8
1. PREAMBLE

The primary objective of the Business Continuity Plan (BCP) is to provide reasonable assurance on the responsiveness or readiness of the Department of Cooperative Governance and Traditional Affairs to manage uncertain future occurrences (risks) that might threaten continued functioning of all spheres of government (Departments, municipalities and other institutions).

2. REGULATORY FRAMEWORK

This policy derives its mandate from the:

a) Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002)
b) Minimum Information Security Standards of 1996
c) State Information Technology Agency (SITA) Act, 2002 (Act No. 38 of 2002)
d) Disaster Management Act, 2002 (Act 57 of 2002)
e) Treasury Regulations as gazetted

3. DEFINITIONS

In this Business Continuity Plan, unless the context otherwise indicates:-

“Accounting Officer” means the Head of Department;

“Business continuity planning (BCP)” means planning which identifies the organization’s exposure to internal and external threats and synthesizes hard and soft assets to provide effective prevention and recovery for the organization, whilst maintaining competitive advantage and value system integrity.

“Disaster recovery” is the process, policies and procedures related to preparing for recovery or continuation of technology infrastructure critical to an organization after a natural or human-induced disaster. Disaster recovery is a subset of business continuity. While business continuity involves planning for keeping all aspects of a business functioning in the midst of disruptive events, disaster recovery focuses on the IT or technology systems that support business functions.

COGTA - Department of Cooperative Governance and Traditional Affairs

IT - Information Technology

SITA - State Information Technology Agency

SAPS - South African Police Services
NIA - National Intelligence Agency
SASS - South African Secret Services
SANDF - South African National Defence Force
PFMA - Public Finance Management Act
AFS - Annual Financial Statements
IEC - Independent Electoral Commission
MTEF - Medium-Term Expenditure Framework
PMG - Paymaster General Account
IYM's - In Year Monitoring
MIG - Municipal Infrastructure Grant

4. **OVERVIEW**

The primary objective of the Business Continuity Plan (BCP) is to provide reasonable assurance on the responsiveness or readiness of Department of Cooperative Governance and Traditional Affairs to manage uncertain future occurrences (risks) that might threaten continued functioning of all spheres of government (Departments, Municipalities and other institutions). A minor computer glitches or theft of money through collusion in one or two departments are taken as minor internal control problems and not something that can threaten the continuity of the provincial since they are fairly manageable. The BCP seeks to address risks in all operational environments which direct bearing on continued functioning of the provincial governments. Disaster Recovery Plans are often confused or used interchangeably with Business Continuity Plans but the reality is the prior is the subset of component of the latter.

The government departments and national industrial facilities are managed and controlled through complex digital networks (complicated and sophisticated computer networks). Growing over reliance on computer systems to run government operations and a must-do transition from manual financial environment to fully integrated and computerised processes (e-commerce) and globalisation in general expose all participants to the shared computer networks to cyber attacks or cyber terrorism. In addition to the cyber attacks and bio terrorism (biological and chemical attacks on water management infrastructure and water sources and deliberate release of deadly bacterium or toxins in public areas) is a reality which is unreal for now.
An attack on our national electricity grid could result in sustained multiple blackouts in all spheres of government in the province and the country as whole. As a result the economy could be affected adversely. Recurring hacking incidents of government business systems and banks is a national security concern- (invite questions on responsiveness or capability of the state to manage the cyber crime conundrum).

The summation of the aforementioned risks are enough to brought the province and country as whole to a standstill since they could affect the transportation sector, waters works, health sector, telecommunications sector, financial sector, energy sector and safety of the citizens. To mitigate the problem or minimise the risks it is imperative to integrated security approach by all government departments, state security agencies and private sector. The approach is necessitated by the fact provincial government does not have full capacity to deal with all forms of risks that threaten its continued existence.

5. **OBJECTIVES OF THE BUSINESS CONTINUITY PLAN**

5.1 To manage the risks pertaining political environment
5.2 To mitigate risks relating to Information Technology (IT) environment
5.3 To manage risks relating Security Management
5.4 To manage risk relating Finance Management and general administration

6. **CURRENT ENVIRONMENT**

The current business environment of the Department of Cooperative Governance and Traditional Affairs (cogta) is segmented into the following:

6.1 **Political environment**
- Political institutions and leadership that runs the government

6.2 **Information Technology environment**
- IT infrastructure and processes

6.3 **Security Management**
- State security agencies supporting political institutions

6.4 **Finance and general administration**
- Physical environment, policies and procedures

6.5 **Social and service delivery environment**
- Electorate at large and service delivery mechanisms or vehicles mobilised to render The service delivery
7. **RISK AND THREAT ANALYSIS**

The risks and threats that might affect the continuity of the provincial government are summarised in tabular format below:

<table>
<thead>
<tr>
<th>No</th>
<th>Environment</th>
<th>Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Political environment</td>
<td>7. Revolt against state due to insensitive political policies</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8. Inadequate service delivery</td>
</tr>
<tr>
<td></td>
<td></td>
<td>9. Ineffective justice system</td>
</tr>
<tr>
<td></td>
<td></td>
<td>10. Lack of accountability and transparency</td>
</tr>
<tr>
<td></td>
<td></td>
<td>11. Unavailability of institutions supporting democracy</td>
</tr>
<tr>
<td></td>
<td></td>
<td>12. Tribalism and Racism</td>
</tr>
<tr>
<td></td>
<td></td>
<td>13. Lack of economic development</td>
</tr>
<tr>
<td></td>
<td></td>
<td>14. High level unemployment</td>
</tr>
<tr>
<td>2</td>
<td>Information Technology environment</td>
<td>• Absence of IT policies and procedures</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Inadequate back systems for government systems</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Inefficiency of the business systems</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Abuse of the business systems</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Lack of security on data files</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Uncontrolled access state IT infrastructure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Inadequate communication system</td>
</tr>
<tr>
<td>3</td>
<td>Security Environment</td>
<td>• Inability to secure international points of entry</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Inability to control access to sensitive state properties – Government complex</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Inability to with organised crime</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Inability to deal espionage activities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Inability to protect its citizen</td>
</tr>
<tr>
<td>4</td>
<td>Finance and General Administration</td>
<td>• Over commitment of government above resources available</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ineffective human capital management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Non compliance with PFMA and Treasury regulations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Ineffective procurement processes</td>
</tr>
<tr>
<td>5</td>
<td>Social and service delivery environment</td>
<td>• Poor service delivery</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Inaccessibility to quality sanitation infrastructure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Inaccessibility to housing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Inadequate roads infrastructure</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Lack of recreational facilities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Lack of disaster facilities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Lack of health facilities</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Shortage of educational facilities</td>
</tr>
</tbody>
</table>
The risk assessments and information gathering processes are carried out by provincial departments, state security agencies and other stake holders to ensure continued functioning of the provincial governments. The institutions and their responsibilities are summarised below:

<table>
<thead>
<tr>
<th>No</th>
<th>Environment</th>
<th>Institutions</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Political environment</td>
<td>The legislature, Premier, National Government, Ruling Party, Other parties, IEC</td>
<td>Responsible of overall functioning of the Department of Cooperative Governance and Traditional Affairs</td>
</tr>
</tbody>
</table>
| 2  | Information Technology Infrastructure | State Information Technology Agency  
Other strategic Stakeholders (Department of Communications, Telkom, Neotel Vodacom, MTN, Cell C, Sentech and private institutions participating in IT and telecommunications industry) | Overall management of the Department of Cooperative Governance and Traditional Affairs's technology infrastructure |
| 3  | Security environment         | Provincial/Departmental Security Units  
South African Police Services  
National Intelligence Agency  
South African Secret Services  
South African National Defence Force  
Other strategic Stakeholders | Overall management of physical access to government facilities, security assessments, Oversee Internal and external security mandates, Manage international points of entries and overall management of territorial integrity of the province and the country as a whole. |
| 4  | Finance and Administration   | Mpumalanga Provincial Treasury  
Auditor General  
Office of the Premier  
Shared Service Units  
Special Investigative Unit  
Public Service Commission  
Public Protector  
Labour Movements  
Other strategic Stakeholders | Overall management of departmental finances and business systems, Overall evaluation on state resources are applied, Reports on the application thereon and recommendations on best practices, policies and interpretations of legislative guidelines |
| 5  | Social and service delivery environment | Provincial departments  
Municipalities  
State Agencies  
Corporate Sector | Responsible for implementation of government programs in line political mandates of the electorate at large |
9. ANALYSIS OF RESPONSIVENESS/CONTINUITY OF DEPARTMENT OF COOPERATIVE GOVERNANCE AND TRADITIONAL AFFAIRS

<table>
<thead>
<tr>
<th>No.</th>
<th>Environment</th>
<th>Continuity Indicators</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 15  | Revolt against state due to insensitive political policies | • The Department of Cooperative Governance and Traditional Affairs and national government have sound and effective political institutions to handle rotation political administration setup.  
• Sound and effective policies, legislative guidelines and legal frameworks are in place to handle political processes.  
• Policies and programmes on economic development, job creation, capacity building and sustainability are in place to address socio economic problems. | 20 Constitution manuals  
21 Policy documents of the ruling party  
22 Provincial Macro Policy plans  
23 Provincial MTEF Plans and performance reports |
| 16  | Inadequate service delivery                      |                                                                                                                                                                                                                       |                          |
| 17  | Ineffective justice system                       |                                                                                                                                                                                                                       |                          |
| 18  | Lack of accountability and transparency          |                                                                                                                                                                                                                       |                          |
| 19  | Unavailability of institutions supporting democracy |                                                                                                                                                                                                                       |                          |
| 24  | Tribalism and Racism                            |                                                                                                                                                                                                                       |                          |
| 25  | Lack of economic development                     |                                                                                                                                                                                                                       |                          |
| 26  | High level unemployment                          |                                                                                                                                                                                                                       |                          |
| 2   | Information Technology environment               | • Absence of IT policies and procedures  
• Inadequate back systems for government systems  
• Inefficiency of the business systems  
• Abuse of the business systems  
• Lack of security on data files  
• Uncontrolled access state IT infrastructure  
• Inadequate communication systems | 27 The Department and SITA has sophisticated and reliable backup systems in place.  
28 Policies and systems manual on systems development, maintenance, and Testing and end user tool kits are in place.  
29 On going accelerated training programs on use of business systems are being conducted.  
30 Effective physical access controls and systems controls are place  
31 Security assessments and cyber security workshops are conducted on a continuous bases | 32 Disaster Recovery Plan developed by Provincial Treasury (Financial Systems)  
33 Systems User manuals  
33.2.1.1 SITA Disaster Recovery |
| 3   | Security Environment                              | • Inability to secure international points of entry  
• Inability to control | • The Provincial Government Complex is manned by government security companies and SAPS round | • Departmental Security Plan  
• Other security directives and |
<table>
<thead>
<tr>
<th>No.</th>
<th>Environment</th>
<th>Continuity Indicators</th>
<th>Reference</th>
</tr>
</thead>
</table>
|     | access to sensitive state properties – Government complex | • Strict physical access controls are enforced  
• On going security assessments conducted on an ongoing bases  
• NIA, SASS and SANDF render additional support where applicable | manual |
| 4   | Over commitment of government above resources available  
• Ineffective human capital management  
• Non compliance with PFMA and Treasury regulations  
• Ineffective procurement processes | • The Department have effective and sound financial management policies, guidelines and monitoring mechanisms in place.  
• Auditor General and Shared Assurance Services Units statutory evaluation or monitoring support. | PFMA, IYMs, PMGs, AFS, Audit reports and Departmental performance reports, Macro Policy Reports |
| 5   | Inaccessibility to quality sanitation infrastructure  
• Inaccessibility to housing  
• Inadequate roads infrastructure  
• Lack of recreational facilities  
• Lack of disaster facilities | Water For All Projects, Disaster Management Facility, MIG infrastructure projects reflect commitment of the Department to discharge its mandates in line with the political aspirations of the electorate. | Consolidated or Provincial Macro Policy reports |

10. TIMING AND MAINTENANCE OF THE BCP

The timing and maintenance of the Departmental BCP is an ongoing process which seeks to assist the Department to adapt to changing circumstances within the environment which it operates.

11. CONCLUSION

The Business Continuity Plan of the Department is sound and not single risks identified as per above mentioned suggest that continuity of the Department is threatened.
12. APPROVAL

The signatories hereof, being duly authorised thereto, by their signatures hereto authorise the execution of the work detailed herein, or confirm their acceptance of the contents hereof and authorise the implementation/adoption thereof, as the case may be, for and on behalf of the parties represented by them.

13. REVIEW OF POLICY

This policy will be reviewed annually or as and when the need arises and it should be in line with legislations and prescripts.

14. CONTRAVENTIONS

Any person who contravenes of fails to comply with any provision of this policy may be subjected to disciplinary action.

THUS DONE AND APPROVED BY THE ACCOUNTING OFFICER

APPROVED/ NOT APPROVED

[Signature]

MR TP NYONI
HEAD: CO-OPERATIVE GOVERNANCE AND TRADITIONAL AFFAIRS

DATE: 31-03-2017