POLICY ON ICT BUSINESS CONTINUITY PLAN / DISASTER RECOVERY
2014/2015
Table of Contents

1. Introduction .................................................................................................................. 2
2. Background ................................................................................................................... 2
3. ICT Business Continuity Goal ....................................................................................... 3
4. Objectives .................................................................................................................... 3
5. Purpose ......................................................................................................................... 4
6. Scope of application ..................................................................................................... 4
7. ICT Continuity Plan Layout ......................................................................................... 4
8. ICT Service Continuity Management Process ............................................................... 5
9. Roles and Responsibilities ............................................................................................ 7
10. Overview of the Departmental Environment in IT Perspective ................................... 8
    11.1 Departmental Business Impact Analysis ................................................................ 11
12. Disaster Recovery Plan ............................................................................................... 15
    12.1 Introduction ............................................................................................................ 15
    12.2 Definition of a Disaster Recovery ......................................................................... 15
1. Introduction

This plan is a systematic process to prevent, predict and manage Information and Communications Technology (ICT) disruption and incidents which have the potential to disrupt ICT services and is planned to result in a more resilient IT service capability aligned to wider departmental requirements.

ICT Business Continuity describes the daily Information and Communications Technology (ICT) activities that are undertaken to enable the department to perform its key functions and deliver its ICT services.

Business Continuity is the term applied to the series of management processes and integrated plans that maintain the continuity of the critical processes of an organization, should a disruptive event take place which impacts the ability of the organization to continue to provide its key services. ICT systems and electronic data are crucial components of the processes and their protection and timely return is of paramount importance.

2. Background

Information and Communication Technology (ICT), in recent years has become integral to many of the essential activities carried out by organizations. The advent of the Internet and other electronic networking services together with the current and developing capabilities of systems and applications has also meant that those organizations have become more and more dependent on reliable, safe and secure ICT infrastructures.

At the same time the need for business continuity management (BCM), including incident preparedness, disaster recovery planning, and emergency response and management, has become steadily more prevalent in developed and developing economies. Failures of supporting ICT services (including information security issues such as systems intrusion and malware infections) are recognized as having the potential to impact the continuity of business operations.

As a result managing ICT and related continuity and other security aspects forms an essential component of business continuity requirements. In addition it is often the case that critical business functions that require business continuity are usually dependent upon ICT. This
dependence means that disruptions to ICT can constitute strategic risks to the reputation of an organization and its ability to operate effectively.

IT Service Continuity is essential for many organizations in the implementation of Business Continuity Management and Information Security Management. It is also essential as part of the implementation and operation of information security management as well as business continuity management as specified in ISO/IEC 27001:2013 and ISO 22301:2012 respectively.

It is therefore critical to develop and implement continuity for the ICT services to help ensure business continuity.

3. ICT Business Continuity Goal

To support the overall Business Continuity Management process by ensuring the required IT technical and service facilities can be resumed with required, and agreed, business timescales. As technology is a core component of most business processes, continued or high availability of ICT is critical to the survival of the business as a whole. This shall be achieved by introducing risk reduction measures and recovery options.

4. Objectives

- Maintain a set of IT Service Continuity Plan and IT recovery that support the overall Business Continuity Plan (BCPs) of the department.
- Complete regular Business Impact Analysis exercise to ensure that all continuity plans are maintained in line with changing business impact and requirements.
- Conduct regular Risk Analysis and management exercises, particularly in conjunction with the business and the availability of management and Security processes, which manage IT services within an agreed level of business risk.
- Provide advice and guidance to all other areas of the business and IT on all continuity – and –recovery related issues.
- Ensure that appropriate continuity and recovery mechanisms are put in place to meet or exceed the agreed business continuity targets.
- Assess the impact of all changes on the IT Service Continuity Plans and Recovery Plans.
• Ensure that proactive measures to improve the availability of services are implemented wherever it is cost – justified to do so.
• Negotiate and agree on the necessary contracts with suppliers for the provision of the required recovery capability to support all continuity plans in conjunction with the Supply Chain Management process.

5. Purpose
The purpose of this policy is to create and maintain a Business Continuity Plan (BCP) for the IT support of critical departmental processes. An effective plan allows the department to minimize the adverse effect of emergencies that arise. The department has an ethical obligation to its workforce, shareholders and customer stakeholders to protect and ensure the continuing operations of the business.

6. Scope of application
This policy encompasses all IT processes and technology that supports critical business functions. The successful implementation of this depends on commitment of senior management and the support of all departmental officials within all spheres of the department and the respective suppliers.

7. ICT Continuity Plan Layout
This plan is based on Impact Awareness method. It shall define the environment, conduct Impact Assessment and Prioritize events according to the business impact and deliver the plan and outline a recovery plan. The plan shall acknowledge the existing departmental policies and strategies.
General Plan Layout Structure/Diagram:

1. Defining the Departmental Environment (IT Perspective)
2. Business Impact / Risk Assessment (Bi/RA)
3. Prioritization of Services
4. Resilience / Continuity Plan

8. ICT Service Continuity Management Process

ICT CONTINUITY MANAGEMENT PROCESS LIFE CYCLE

1. Initiation
2. Requirements and Strategy
3. Implementation
4. Ongoing Operation
8.1 Key Activities:

- **Initiation**
  - Policy setting
  - Scope
  - Initiate a project

- **Requirements and Strategy** (Business Continuity Strategy)
  - **Business Impact Analysis (BIA)** - to quantify the impact of loss that IT service would have on business.
  - **Risk Assessment (RA)** - Identify potential threats to continuity and the likelihood of the threats becoming reality. This also includes taking measures to manage the identified threats where this can be cost-justified.
  - **IT Service Continuity Strategy** – Production of overall strategy that must be integrated into Business Continuity Management Strategy. It can produce the two steps identified above, and is likely to include the elements of risk reduction as well as selection of appropriate and comprehensive recovery options.

- **Implementation** (Business Continuity Plans)
  - Develop IT Service Continuity Plans
  - Develop IT Plan, Recovery plans and procedures
  - Organization Planning
  - Testing Strategy

- **Ongoing operation** (Invocation)
  - Education, awareness and Training
  - Review and Audit
  - Testing
  - Change Management
9. Roles and Responsibilities

It is the responsibility of ICT Manager to ensure that the aim of IT Service Responsibilities is met. This shall include such tasks and responsibilities as:

- Performing Business Impact Analysis for all existing and new services.
- Implementing and maintaining the ICT continuity process in accordance with the overall requirements of the department's Business Continuity Management process, and representing the IT Services function within the Business Continuity Management process.
- Ensuring that all ICT Continuity plans, risks and activities underpin and align with all Business Continuity Management plans.
- Performing Risk assessment and risk management to prevent disasters where cost-justified and practical.
- Assessing the potential service continuity issues and invoking the Service Continuity Plan if necessary.
- Managing the Service Continuity Plan while it is in operation, including fall -over to a secondary location and restoration to the primary location.
- Performing post mortem review of service continuity tests and invocations, and instigating corrective actions where required.
- Developing and managing the ICT continuity plans to ensure that, at all times, the recovery objectives of the business can be achieved.
- Ensuring that all IT service areas are prepared and able to respond to an invocation of the continuity plans.
- Undertaking regular reviews, at least annually, of the Continuity Plans with the business areas to ensure that they accurately reflect the business needs.
- Negotiating and managing contracts with providers of third-party recovery services.
- Assessing changes for their impact on Service Continuity and Continuity Plan.
10. Overview of the Departmental Environment in IT Perspective

The department does not own any network infrastructure, as such all the departmental ICT application systems are hosted at Office of the Premier. Amongst other services, ICT in the department in terms of network infrastructure is limited to Desktop Support, Service Level Agreement, and Configuration Management etc. ICT in the department shall ensure that departmental data is secured from user End-Point and also ensure IT Service Continuity from technical support perspective.

The following are transversal systems which are indirectly referred to in this plan, and shall be managed through Service Level Agreement (SLA):

i) Basic Accounting System (BAS) – Financial System  
ii) GroupWise – Email System  

(iii) PERSAL – Personnel Salary System  

iv) Filr – File Backup System  

v) Remedy System – Technical System  

vi) WALKER – Financial System  

Key Departmental Core Business Application Systems which are also referred to in this plan with the same SLA terms as above include:

i) Housing Subsidy System (HSS)  

ii) IMMIS (Integrated Municipal Management Information System)  

In the event of an incident, the plans and systems in place should ensure a resumption of service within the agreed Service Level Agreements (SLAs) ensuring compliance and customer satisfaction as well as aiding in Business Continuity. This plan shall indirectly also include departmental data stored in the following formats:

i) Doc – Word Documents  

ii) xls – Excel Documents  

iii) PDF – Acrobat Reader/Adobe files  

iv) Ppt – Power Point Files  

v) Archive Files (email files)

The above mentioned Business Application System shall be assessed as follows:

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Severity</th>
<th>Negligible (1)</th>
<th>Minor (2)</th>
<th>Moderate (3)</th>
<th>Major (4)</th>
<th>Extreme (5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rare (1)</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td>Unlikely (2)</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>Possible (3)</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td></td>
</tr>
<tr>
<td>Likely (4)</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>Very High</td>
<td></td>
</tr>
<tr>
<td>Almost certain (5)</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>Very High</td>
<td>Very High</td>
<td></td>
</tr>
</tbody>
</table>

Criteria and Risk categories for the identification and classification of Risk:

**IMPACT:**

<table>
<thead>
<tr>
<th>SCORE</th>
<th>RATING</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Catastrophic</td>
<td>Loss of ability to sustain ongoing operations. A situation that would cause a standalone business to cease operation.</td>
</tr>
<tr>
<td>4</td>
<td>Major</td>
<td>Significant impact on achievement of strategic objectives and targets relating to the departmental plan.</td>
</tr>
<tr>
<td>3</td>
<td>Moderate</td>
<td>Disruption of normal operations with a limited effect on achievements of strategic objectives or targets relating to departmental plan.</td>
</tr>
<tr>
<td>2</td>
<td>Minor</td>
<td>No material impact on achievement of the departmental strategies or objectives.</td>
</tr>
<tr>
<td>1</td>
<td>Insignificant</td>
<td>Negligible impact.</td>
</tr>
</tbody>
</table>
### Likelihood:

<table>
<thead>
<tr>
<th>Score</th>
<th>Rating</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Almost Certain (Common)</td>
<td>The risk is almost certain to occur more than once within the next 12 months. (Probability = 100% p.a.)</td>
</tr>
<tr>
<td>4</td>
<td>Likely</td>
<td>The risk is almost certain to occur once within the next 12 months. (Probability = 10-50% p.a.)</td>
</tr>
<tr>
<td>3</td>
<td>Moderate</td>
<td>The risk could occur at least once in the next 2 – 10 years. (Probability = 10 – 50 % p.a.)</td>
</tr>
<tr>
<td>2</td>
<td>Unlikely</td>
<td>The risk could occur at least once in the next 10 – 100 years; (Probability = 1 – 10% p.a.)</td>
</tr>
<tr>
<td>1</td>
<td>Rare</td>
<td>The risk shall probably not occur, i.e. less than once in 100 years. (Probability = 0 -1% p.a.)</td>
</tr>
</tbody>
</table>

Risk Assessment ratings are the product of likelihood and impact and are ranked as follows:

<table>
<thead>
<tr>
<th>From 15 - 25</th>
<th>Very High</th>
</tr>
</thead>
<tbody>
<tr>
<td>From 11- 14</td>
<td>High</td>
</tr>
<tr>
<td>From 5 – 10</td>
<td>Medium</td>
</tr>
<tr>
<td>From 1 - 4</td>
<td>Low</td>
</tr>
</tbody>
</table>
## 11.1 Departmental Business Impact Analysis

<table>
<thead>
<tr>
<th>Location/Hosting</th>
<th>Departmental ICT System</th>
<th>Type of Loss/ Damage</th>
<th>Likelihood</th>
<th>Severity</th>
<th>Business Impact</th>
<th>Financial Implications</th>
<th>Recovery Time</th>
<th>Precautions in place</th>
</tr>
</thead>
</table>
| SITA Building    | BAS                     | • Loss of ICT Equipments  
• Data loss  
• Fire  
• Flash flood  
• Pandemic (Virus attacks)  
• Power Outage  
• War  
• Theft  
• Terrorist Attack | 5 | 4 | Disruption of normal operations with a limited effect on achievements of strategic objectives or targets relating to departmental plan. | None | 24-48 hours |
| Garona Building  | PERSAL                  | • Loss of ICT Equipments  
• Data loss  
• Fire  
• Flash flood  
• Pandemic (Virus attacks)  
• Power Outage  
• War  
• Theft  
• Terrorist Attack | 5 | 4 | Disruption of normal operations with a limited effect on achievements of strategic objectives or targets relating to departmental plan. | None | 24-48 hours |
<p>| Garona Building  | WALKER                  | 5 | 4 | Disruption of normal | None | 24-48 |</p>
<table>
<thead>
<tr>
<th>Building</th>
<th>System</th>
<th>5</th>
<th>4</th>
<th>Description</th>
<th>Units</th>
</tr>
</thead>
<tbody>
<tr>
<td>Garona</td>
<td>GroupWise</td>
<td></td>
<td></td>
<td>Disruption of normal operations with a limited effect on achievements of</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>strategic objectives or targets relating to departmental plan.</td>
<td></td>
</tr>
<tr>
<td>Gai</td>
<td>Remedy</td>
<td></td>
<td></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5 days</td>
<td></td>
</tr>
<tr>
<td>Garona</td>
<td>Filr</td>
<td></td>
<td></td>
<td>Disruption of normal operations with a limited effect on achievements of</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>strategic objectives or targets relating to departmental plan.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>None</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>15 minutes</td>
<td></td>
</tr>
<tr>
<td>Location/Hosting</td>
<td>Departmental ICT System</td>
<td>Type of Loss/ Damage</td>
<td>Likelihood</td>
<td>Severity</td>
<td>Business Impact</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------</td>
<td>-------------------------------------------------------------------------------------</td>
<td>------------</td>
<td>----------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Telkom Building</td>
<td>Word, Excel, PowerPoint, PDF, Email Archives</td>
<td>Fire, Theft, Water Damage, Vandalism, Virus attack and Terrorist attack</td>
<td>3</td>
<td>4</td>
<td>Poor decision making and inadequacy of information as a result of missing files. Business might have to regenerate data at the expense of departmental time. Poor service delivery in terms of time and money.</td>
</tr>
<tr>
<td>CCP Building</td>
<td>Word, Excel, PowerPoint, PDF, Email Archives</td>
<td>Fire, Theft, Water Damage, Vandalism, Virus attack and Terrorist attack</td>
<td>3</td>
<td>4</td>
<td>Poor decision making and inadequacy of information as a result of missing files. Business might have to regenerate data at the expense of departmental time. Poor service delivery in terms of time and money.</td>
</tr>
<tr>
<td>NWDC</td>
<td>HSS</td>
<td></td>
<td>3</td>
<td>4</td>
<td>Disruption of normal operations, Poor decision making and inadequacy of information as a result of missing files. Business might have to regenerate data at the expense of departmental time. Poor service delivery in terms of time and money.</td>
</tr>
<tr>
<td>NWDC Building</td>
<td>Word, Excel, PowerPoint, PDF, Email Archives</td>
<td>Fire, Theft, Water Damage, Vandalism, Virus attack and Terrorist attack</td>
<td>3</td>
<td>4</td>
<td>Poor decision making and inadequacy of information as a result of missing files. Business might have to regenerate data at the expense of departmental time. Poor service delivery in terms of time and money.</td>
</tr>
</tbody>
</table>
12. DISASTER RECOVERY PLAN

12.1 Introduction
This Disaster Recovery Plan captures, in a single repository, all of the information that describes the Department's ability to withstand ICT disaster as well as the processes that must be followed to achieve disaster recovery.

12.2 Definition of a Disaster Recovery
This is the process, policies and procedures that are related to preparing for recovery or continuation of technology infrastructure, which are vital to the Department after a natural or human-induced disaster. It focuses on the IT or technology systems that support business functions.

A disaster can be caused by man or nature and results in the department not being able to perform all or some of their regular roles and responsibilities for a period of time. In this document a disaster is defined as follows:

- One or more vital systems are non-functional
- The building is available but systems are non-functional
- The building and all systems are non-functional

The following events can result in a disaster, requiring this Disaster Recovery document to be activated:

- Loss of ICT Equipments
- Data loss
- Fire
- Flash flood
- Pandemic (Virus attacks)
- War
- Theft
- Terrorist Attack
12.3 Purpose

The purpose of this DRP document is in twofold: first to capture all of the information relevant to the Department’s ability to withstand a disaster, and second to document the steps that the department shall follow if a disaster occurs.

Note that in the event of a disaster the first priority of the ICT unit is to prevent the loss of data.

This DRP takes all of the following areas into consideration:

- Data Storage and Backup Systems
- End-user Computers
- IT Documentation

This DRP does not take into consideration any non-IT, personnel, Human Resources and real estate related disasters.
12.4 Scope of application

This plan is confined to user data recovery in the format as outlined above.

12.5 Version Information & Changes

Any changes, edits and updates made to the DRP shall be recorded in here. It is the responsibility of the Disaster Recovery Lead to ensure that all existing copies of the DRP are up to date. Whenever there is an update to the DRP, the Department requires that the version number be updated to indicate this.

<table>
<thead>
<tr>
<th>Name of Person Making Change</th>
<th>Role of Person Making Change</th>
<th>Date of Change</th>
<th>Version Number</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

12.6 Disaster Recovery Teams & Responsibilities

In the event of a disaster, the following are key stakeholders who shall be required to restore normal functionality to the employees of the Department.

- Disaster Recovery Leads (Disaster management Directorate, GITO)
- Disaster Recovery Team (ICT Unit)
- ICT Steering Committee
- ICT Operational Committee
12.6.1 Disaster Recovery Lead

The Disaster Recovery Lead shall oversee the entire disaster recovery process and is responsible for making all decisions related to the Disaster Recovery efforts. He/she shall be the first person to take action in the event of a disaster. This person shall evaluate the disaster and shall determine what steps need to be taken to get the department back to business as usual.

This person's primary role shall be to guide the disaster recovery process and all other individuals involved in the disaster recovery process shall report to this person in the event that a disaster occurs in the Department, regardless of their business unit and existing managers. All efforts shall be made to ensure that this person be separate from the rest of the disaster management teams to keep his/her decisions unbiased; the Disaster Recovery Lead shall not be a member of other Disaster Recovery groups in the Department. The Disaster Recovery Lead shall report to the Management Team.

12.6.1.1 Roles and Responsibilities

- Make the determination that a disaster has occurred and trigger the DRP and related processes.
- Be the single point of contact for and oversee all of the DR Teams.
- Organize and chair regular meetings of the DR Team leads throughout the disaster.
- Present to the Management Team on the state of the disaster and the decisions that need to be made.
- Organize, supervise and manage all DRP test and author all DRP updates.
- Set the DRP into motion after the disaster has been declared.
- Determine the magnitude and class of the disaster
- Determine what systems and processes have been affected by the disaster
- Communicate the disaster to the other disaster recovery teams
• Determine what first steps need to be taken by the disaster recovery teams
• Keep the disaster recovery teams on track with pre-determined expectations and goals
• Keep a record of incidents and money spent during the disaster recovery process
• Ensure that all decisions made abide by the DRP and policies set by the Department
• Get the secondary site ready to restore business operations
• Ensure that the secondary site is fully functional and secure
• Create a detailed report of all the steps undertaken in the disaster recovery process
• Notify the relevant parties once the disaster is over and normal business functionality has been restored

Contact Information

<table>
<thead>
<tr>
<th>Name</th>
<th>Role/Title</th>
<th>Work Phone Number</th>
<th>Mobile Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disaster Management</td>
<td>Director</td>
<td>0183884446</td>
<td>0834543350</td>
</tr>
<tr>
<td>GITO</td>
<td>Primary Disaster Lead</td>
<td>0183882423</td>
<td>0836760026</td>
</tr>
</tbody>
</table>

12.6.2 Disaster Recovery Team

This team shall oversee the entire disaster recovery process. They shall be the first team that shall need to take action in the event of a disaster. This team shall evaluate the disaster and shall determine what steps need to be taken to get the department back to business as usual.

12.6.2.1 Role & Responsibilities

• Set the DRP into motion after the Disaster Recovery Lead has declared a disaster
• Determine the magnitude and class of the disaster
• Determine what systems and processes have been affected by the disaster
- Communicate the disaster to the other disaster recovery teams
- Determine what first steps need to be taken by the disaster recovery teams
- Keep the disaster recovery teams on track with pre-determined expectations and goals
- Keep a record of money spent during the disaster recovery process
- Ensure that all decisions made abide by the DRP and policies set by the Department
- Get the secondary site ready to restore business operations
- Ensure that the secondary site is fully functional and secure
- Create a detailed report of all the steps undertaken in the disaster recovery process.
- Notify the relevant parties once the disaster is over and normal business functionality has been restored.

- After the Department is back to business as usual, this team shall be required to summarize any and all costs and shall provide a report to the Disaster Recovery Lead summarizing their activities during the disaster.

**Contact Information**

<table>
<thead>
<tr>
<th>Name</th>
<th>Role/Title</th>
<th>Work Phone Number</th>
<th>Mobile Phone Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICT Unit</td>
<td>AD: ICT</td>
<td>0183882228</td>
<td>0788029361</td>
</tr>
<tr>
<td>HSS Unit</td>
<td>DD: HSS</td>
<td>0183885543</td>
<td>0790706555</td>
</tr>
<tr>
<td>IMMIS</td>
<td>DD: Reporting and Data Management</td>
<td>0183883514</td>
<td>0714704627</td>
</tr>
<tr>
<td>Disaster Management</td>
<td>DD: Information Management and Communications System</td>
<td>0183885232</td>
<td>072878502</td>
</tr>
</tbody>
</table>

**12.6.3 ICT Operational Committee**

This team's primary goal shall be to provide employees with the tools they need to perform their roles as quickly and efficiently as possible. They shall need to provide all the departmental