LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
COOPERATIVE GOVERNANCE,
HUMAN SETTLEMENTS & TRADITIONAL AFFAIRS

IT Continuity Policy

Version: 2

Version Control

Version	Date	Author(s)	Details
1.0 - Original	10/11/2008	Moloko Monyepao	Original draft developed by SITA
2.0 draft	06/03/2014	Samuel Mantlaka	Policy transfer from SITA to CoGHSTA format
2.0 final	12/03/2014	Samuel Mantlaka	Adopted by Labour Management Forum

Table of Contents

I. Acronyms and Abbreviations

CoGHSTA	Co-Operate Governance, Human Settlements, and Traditional Affairs
DGITO	Departmental Government Information Technology Officer
DRP	Disaster Recovery Plan
HoD	Head of Department
IT	Information Technology
MISS	Minimum Information Security Standard
SBU	Strategic Business Unit
SITA	State Information Technology Agency
Sub-dept	Sub Department

1. Preamble

This policy document will provide an overall policy that governs IT Continuity/Disaster Recovery within the Department of Co-Operative Governance, Human Settlements and Traditional Affairs. IT Continuity Management is a continuous process of risk assessment and risk management with the purpose of ensuring that CoGHSTA can continue to deliver its key services should a disruption arise. A disruption can arise when threat materializes during the course of our normal service delivery.

IT Recovery starts by carefully agreeing to business units requirements and determining the cost of downtime or unavailability of the specific service in question, so that a realistic disaster recovery requirement can be established

This process involves an element of awareness creation and consensus among all parties involved. To be successful in this regard, CoGHSTA would need to understand how to defineand present its requirements.

IT Continuity is a business requirement to enable the recovery of data and applications in the case of events such as natural disasters, system disk drive failures, espionage, data entry errors, and system errors.

2. Purpose and objectives

The purpose of this policy is for the CoGHSTA to have the capacity to resume operational effectiveness within a specified period of time after the onset of a disaster or other disrupting events.

The secondary objectives are as follows:

2.1. Staff welfare and confidence during and after a disaster incident

2.2. Continuous service delivery to people of Limpopo

2.3. Maintenance of client and CoGHSTA stakeholder contact and confidence

2.4. Fulfilment of regulatory requirements

2.5. Control expenditure and lower costs caused by the disaster incident

2.6. Apply the CoGHSTA Risk Management framework to priority areas

3. Scope of Application

This policy, except otherwise indicated, is applicable to all employees (including service providers, contractors and temporary staff) utilizing departmental ICT systems across CoGHSTA networks.

4. Legal Framework

The following publications govern the execution of the IT Continuity policy and were taken into consideration during the drafting of the DRP:

4.1. SABS/ISO 25999

4.2. SABS/ISO 17799

4.3. Minimum Information Security Standards

4.4. Protection of Information Act 4 of 2013

4.5. Public Service Act 30 of 2007

4.6. Regulation of Interception of Communications Act 36 of 2005

4.7. COBIT Audit framework

4.8. Electronic Communications and Transactions Act 25 of 2002

5. Administration of the policy

GITO is responsible for enforcing this policy and continuously ensuring monitoring and compliance.

6. Policy Authority

6.1 The HOD is and remains responsible for the overall IT Continuity Policy. This responsibility is delegated to DGITO.

6.2 It is the responsibility of the business units (Sub-dept, Branch, SBU, Division and units) to ensure that they have enough information in their specific section of the IT Continuity Plan, to enable them to recover from a disaster and continue to provide a service to clients within acceptable timeframes.

7. Policy Contents

7.1. Policy Statement

7.1.1. All IT staff responsible for performing IT Continuity activities and procedures will follow the IT Recovery process as documented: An initial Risk Assessment must be undertaken in order to determine the requirements for the IT Continuity Plan.

7.1.2. The Department should have in place an approved comprehensive Disaster Recovery Plan to ensure that it can recover all critical IT and information systems in the event of a disaster.

7.1.3. It is management's objective that all business units within CoGHSTA have detailed IT Continuity Plans to ensure that all critical processes can be continued in the event that a serious unplanned event occurs, which may disrupt the normal execution of those processes.

7.1.4. The collection of individual business unit IT Continuity Plans will form the CoGHSTA IT Continuity Plan. It is the responsibility of all business unit management to assist in the development and support of this plan and to ensure that their individual IT Continuity Plans conform to the overall standard as prescribed by the IT Continuity planning team.

7.1.5. The IT Continuity Plan should cover all essential and critical business activities which relate to its daily operations. In the event of a disaster, it must be possible for the Department to continue operating even at limited capacity.

7.1.6. The IT Continuity Plan should be periodically tested at pre-determined dates or on ad hoc basis to ensure that it can be implemented in an emergency situation, and that management and staff understands what is required for execution.

7.1.7. The IT Continuity Plan should be kept up to date to take into account any relevant change within the Department's IT and information systems environment.

7.1.8. Staff should be made aware of the IT Continuity Plan and their specific roles (if applicable) defined within the plan.

7.2. Business Units Responsibilities

In order to support the above objective fully, all business units are expected to ensure that:

7.2.1. They identify their critical business processes, functions and outputs ;

7.2.2. They identify and assess any threats to those business processes, functions and outputs;

7.2.3. They put in place measures to eliminate those threats, or if it is not possible, develop plans to mitigate and manage them, should they materialize;

7.2.4. They comply fully with all the requirements of this IT Continuity Management Policy;

7.2.5. Evaluate and recommend strategies for the reduction or transfer of risk (including appropriate insurance, where available);

7.2.6. Develop the IT Continuity strategy consistent with the organisation's overall business and security strategy;

7.2.7. Regularly test, review, and update all procedures relating to the IT Continuity Plan;

7.2.8. Ensure IT Continuity Planning is integrated into business functions and daily operations;

7.2.9. Allocate responsibility to individuals in their business units to fulfil the requirements of the IT Continuity plan; and

7.2.10. Ensure that records are managed in accordance with the Departmental Records Management Policy and that all the required IT Continuity documentation and records are available and current.

7.3. Key Risk Areas

The key areas that can affect our delivery of service as at the time of writing this policy are as follows:

7.3.1 The denial of access to CoGHSTA facilities due to, for example:-

7.3.1a Vandalism

7.3.1b Accidental fire or arson

7.3.1c Scene of crime investigation

7.3.1d Dangerous structures

7.3.1e Flooding

7.3.2 Staff shortages due to, for example:-

7.3.2a Loss of key staff/skills

7.3.2b Industrial action

7.3.2c Fuel shortage

7.3.2d Prolonged severe weather

7.3.2e A major influenza outbreak

7.3.3 Denial of service due to for example:-

7.3.3a Failure of a supporting service such as:-

7.3.3b Computing system fails

7.3.3c A sub-contractor's business fails

7.3.3d Telephone system fails

7.3.3e Unavailability of proprietary and critical information

7.4 IT Continuity Scope

The IT Continuity Management (Disaster Recovery) policy covers all the functions contained within CoGHSTA. It forms the basis for all IT Continuity Planning activities. It is expected that the implementation of IT Continuity Management Plan within CoGHSTA will follow the guidelines and processes outlined in PAS77 (IT Continuity) AND BS25999 (Business Continuity) standards.

7.5 Key Role Players and Responsibilities

In order for Disaster Recovery to be successful, the following input requirements are essential:

7.5.1. Internal:

7.5.1.1. Change Management – Changes to the IT Infrastructure need to be reviewed for impact and risk to on-going Disaster Recovery requirements.

7.5.1.2. ICT Manager – The manager (ICT) through the guidance from the IT Steering Committee is currently responsible for defining and maintaining the framework for IT Continuity Management which includes policy, strategy, overall implementation, plan documentation structure, provision of business and support unit templates, tests and training requirements, review and change management requirements as well as initiating tests and reviews.

7.5.1.3. Financial Management – IT Continuity works closely with Financial Management to fully understand the cost of delivery required by Disaster Recovery at justified costs. IT Recovery will also provide budget information based on an annual Recovery Plan.

7.5.1.4. Security Management - Security requirements are taken into account in the IT Recovery design activities.

7.5.1.5. Service Level Management - Service Level Management (SLM) helps define the Business Requirements for IT Recovery. SLM will also help in identifying the Vital Business Functions. SLM also plays a major role in the actual reporting of Disaster Recovery achievements on a consistent basis. SLM also provides IT Recovery information on Underpinning Contracts.

7.5.1.6. Incident Management - Incident data is used as an input to IT recovery and planning activities.

7.5.1.7. Support Units - It is the responsibility of the support units to ensure that they have enough information in their specific section of the IT Continuity Plan, to enable IT to recover the infrastructure and services required to support business recovery activities within acceptable timeframes.

7.5.2. External:

7.5.2.1. All 3rd Party Vendors

7.6 IT Continuity Management Process

7.6.1. The IT Continuity Management process shall consist of four stages:

Stage 1: Planning
Stage 2: Implementation and Operation of IT Continuity Strategy
Stage 3: Monitor and Review
Stage 4: Maintenance and Improvement

The first two stages involve the establishment and implementation of IT Continuity Management within CoGHSTA. The final two stages ensure an ongoing operational management of the process.

Stage 1: Planning

This stage covers the establishment of the IT Continuity Management process, including sponsorship, budget approval and identification of appropriate resources.

Stage 2: Implementation and Operation of IT Continuity Strategy

This stage provides the foundation for IT Continuity Management and is critical to determine:

2a How well CoGHSTA will survive an IT interruption or disaster.

2bAny costs that will be incurred as a result of a business interruption or disaster.

2cRequirements identified through the Business Impact Analysis and Risk Assessment activities.

2d The outputs from the above activities that will feed into the IT Continuity Management strategy, which proposes risk reduction measures and recovery options, in support of business continuity.

2e Once the IT Continuity Strategy has been agreed, the IT Continuity Management lifecycle will move into the actual implementation activities. These activities will include:

1. Establishing a IT Continuity Management Plan with clear roles and responsibilities for any personnel who will be involved in a recovery

2. Developing Training, awareness and competency plans
3. Developing implementation and supporting plans
4. Developing and implementing an incident response structure
5. Providing resources to implement risk reduction measures that are detailed in the IT Continuity Strategy
6. Procuring recovery facilities
7. Proving continuity capability through initial testing
8. Embedding IT Continuity in the CoGHSTA culture
9. Developing and implementing change management procedures
10. Testing of the IT Continuity Plan
11. IT Continuity documentation and records management

Stage 3: Monitor and Review

3a The completion of the first two stages of the IT Continuity Management process will mean that an IT Continuity Management solution has been analysed, agreed and implemented within the organisation.

3b CoGHSTA facilities will then need to ensure that the strategy and recovery are maintained as part of day-to-day business activities.

3c DGITO has responsibility for maintaining the IT Continuity Management environment through a series of operational management activities.

These activities will include:

- Internal and External reviews – each business unit will be responsiblefor reviewing their own IT Continuity activities at agreed time intervals. The GITO Management will ensure that IT Continuity Plan is tested either on an ad hoc basis or at planned intervals.

- Management reviews of the IT Continuity Plan – The test results from above will feed into the management review of the IT Continuity Plan. The decisions and actions recommended by management will feed into the Maintenance and Improvement stage.

Stage 4: Maintenance and Improvement

4a The completion of stage three will mean that the status of IT Continuity Plan at CoGHSTA will have been established and there could be need for improvement and making changes to suit the current requirements of CoGHSTA.

4b CoGHSTA will document all procedures for corrective and preventative action to ensure that the CoGHSTA IT Continuity Plan conforms to the PAS77 AND BS25999 standard. All such procedures, minutes, records pertaining to the IT Continuity Plan will form part of the CoGHSTA IT Continuity records and documentation as required by the PAS77 AND BS25999 standard.

7.7 Offsite and Backup Storage

7.7.1. All users using desktop applications will be required to comply with the CoGHSTA "My Document" roaming profile procedures.

7.7.2. The frequency and extent of backups must be in accordance with the importance of the information and the acceptable risk as determined by the data owner.

7.7.3. CoGHSTA Information Resources backup and recovery process for each system must be documented and periodically reviewed.

7.7.4. Offsite backup storage facilities for CoGHSTA will be handled by SITA.

7.7.5. Physical access controls implemented at offsite backup storage locations must meet or exceed the physical access controls of the source systems.

Additionally backup media must be protected in accordance with the highest CoGHSTA sensitivity level of information stored. This shall be as determined in respect to MISS.

7.7.6. A process must be implemented to verify the success of CoGHSTA electronic information backup.

7.7.7. Backups must be periodically tested to ensure that they are recoverable.

7.7.8. Signature cards held by the offsite backup storage vendor(s) for access to CoGHSTA backup media must be reviewed annually or when an authorized individual leaves CoGHSTA.

7.7.9. Procedures between CoGHSTA and SITA must be reviewed at least annually.

7.7.10. Backup media in transit shall comply with all the requirements of section 7.7.2 of the Information Management and Electronic Security standard. In addition to meeting these requirements the backup media shall be encrypted to ensure that its protection against unauthorized access.

7.7.11. The identification of Backup tapes shall comply with section 7.7.4 of the Information Management and Electronic Security Standard.

8. Default

Non-compliance of this policy shall constitute violation of the policy and shall be treated in terms of the Departmental Disciplinary Code and Procedure Policy.

9. Adoption of the Policy

This policy shall be considered and adopted by the Labour Management Forum.

10. Inception Date

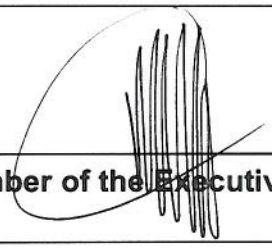
This policy comes into effect from the date of approval by Member of Executive Council.

11. Policy Review

This policy shall be reviewed bi-annually.

12. Enquiries

Enquiries about the policy should be directed to the Government Information Technology Office.

Document Title	**IT Continuity Policy**
Compiled by :	**Government Information Technology Office**  **Senior Manager** **(ICT Infrastructure and Systems)** 19/03/2014 **Date**
Acknowledge by :	 **General Manager (GITO)** 20/03/2014 **Date**
Recommended by:	 **Senior General Manager** **(Corporate Services)** 01/04/14 **Date**
Adopted by :	 **Head of Department** 03/04/2014 **Date**
Approved by :	 **Member of the Executive Council** 1d/04/2014 **Date**