Province of the
EASTERN CAPE
COOPERATIVE GOVERNANCE
& TRADITIONAL AFFAIRS

INFORMATION AND COMMUNICATION TECHNOLOGY DISASTER RECOVERY POLICY

Departmental Contact Details	
Physical Address	**Tyamzashe Building** **Phalo Avenue** **Bhisho** **5605**
Postal Address	**Department of Cooperative Governance and Traditional Affairs** **Private Bag X0035** **Bhisho** **5605**
Document Number	**CGICT-DRPOL-001**
Document Name	**ICT Disaster Recovery Policy**
Custodian	**Ms T.M. Luke**
Designation	**Director: Government Information Communication and Technology Management**
Component	**Government Information Communication and Technology Management (GICTM)**
Telephone No.	**040 940 7235**
Cell Phone No.	**076 141 1749**
E-mail Address	**tswakai.luke@eccogta.gov.za**
Date Completed	
Date of Approval	
Date Last Amended	
Related Policies	Disaster recovery Plan ICT Security Policy ICT User Access Management Policy Information Communication & Technology Data Backup & Recovery Policy & Procedures

SIGN OFF

HEAD OF DEPARTMENT

The Disaster Recovery Policy has been recommended by Mr. V. Mlokothi in my capacity as the Head of the Eastern Cape Department of Cooperative Governance and Traditional Affairs (DCoGTA).

I am satisfied and concur with the contents of this Policy.

The development of the policy on Disaster Recovery will ensure the department is able to exercise its powers in compliance with the law and guide decision- making in the department.

Signed	
Designation	Mr. V. Mlokothi, Head of Department: Cooperative Governance and Traditional Affairs
Date	10/08/2025

Executive Authority

The Department of Cooperative Governance and Traditional Affairs has an unprecedented opportunity to improve the livelihoods of the people by effectively rendering the many services that it is expected to provide. We have envisaged a department that has the required capacity to respond adequately to the challenges of its people.

I therefore trust that guidance from this Disaster Recovery Policy will contribute to the effective fulfilment of the departmental mandate, the service delivery expectations of the public and the performance expectations within the department.

Signed	
Designation	Member of the Executive Council : Honourable Z.A. Williams of Cooperative Governance and Traditional Affairs
Date	12.08.2025

Contents

1. ABBREVIATIONS AND DEFINITIONS

TERM	DEFINITION
Abbreviations	
AD	Active Directory
Ad hoc	As and when requested.
COGTA	Department of Cooperative Governance and Traditional Affairs
Directorates	Chief Directorates/Directorates
DR	Disaster Recovery
GICTM	Government Information and Communication Technology Management
HOD	The Head of Department
HR	Human Resources
LAN	Local Area network
UI	User Information
VM	Virtual Machine
Definitions	
Availability	The proportion of time a system is in a functioning condition.
Business Continuity	A plan that will enable the Business Unit to resume an acceptable level of service in an acceptable time frame, after a disaster has occurred.
Critical data	Data that is required to be retained for a set period as determined by law, or data that can severely disrupt services when lost. Examples include financial data, user personal data etc.
Critical Time Frame	The critical time frame for a Business Unit is the elapsed time from the point where a disruption in computer services occurred, up to the time when critical losses will start occurring because of the unavailability of computer-driven business processes.
Data referencing	Data that defines the set of permissible values to be used by other data sets.
Disaster	A disaster event that adversely impacts on COGTAs ability to process, provide, or utilize information essential to its strategic day-to-day operations or which causes an inability within COGTA to provide users with basic services. The term "disaster" includes a failure or a loss (whole or partial) of equipment/systems/software (including human resources) from whatever cause including but not limited to equipment failure, industrial action, illness, conflagration, explosion, earthquake, tornado, flood, subsidence, collapse, riot, contamination by water/smoke/chemicals and/or otherwise.
Disaster Recovery	The process of reconstructing the current information technology used by a Business Unit if the original system(s) is/are rendered inoperable, non-recoverable and/or inaccessible.
Downtime	Defined as the periods when a system is unavailable.

TERM	DEFINITION
HEAD OF ICT	The ICT Director, also referred to as Government Information Technology Officer (GITO)
Integrity	Data integrity is defined as the assurance that data is consistent and correct.
Operational Recovery	The process whereby problems affecting production computer systems are resolved and the computer systems reinstated at the production site. Should the estimated operational recovery time exceed the critical time frame, as stipulated in the disaster recovery plan, a disaster can be declared.
SAN	Storage Area Network, a device that has large amounts of space
Secondary Backup Facility	A secondary backup facility is an additional facility that could stand in for failure of the normal first line (primary) backup facilities.
Storage capacity	Amount of space (TB Terabyte; GB Gigabyte; MB Megabyte, KB Kilobyte) utilized
Virtual Machine	A software machine that is hosted by a physical host
Worst Case Scenario	For implementation of the organizational Disaster Recovery Policy, a worst-case scenario is regarded as the destruction/loss of computer systems (hardware and software) for any cause whatsoever.

Table 1 - Abbreviations and Definitions

2. EXECUTIVE SUMMARY

This Disaster Recovery Policy outlines the strategic framework and operational procedures to ensure the continuity and rapid recovery of critical business functions in the event of a disruptive incident. The policy is designed to minimise downtime, protect departmental assets, and maintain service delivery to clients and stakeholders.

3. INTRODUCTION

This policy document will provide an overall policy that governs IT Continuity/Disaster Recovery within the Department. IT Continuity Management is a continuous process of risk assessment with the purpose of ensuring that COGTA can continue to deliver its key services should a disruption arise. A disruption can arise when a threat materialises during the course of normal service delivery.

IT Recovery starts by carefully determining the cost of downtime or unavailability of the specific service in question, so that a realistic disaster recovery requirement can be established. 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, or system operations errors, terrorism, sabotage, malicious damage, theft, robbery etc.

Disaster Recovery Planning is the section that deals with the restore and recovery processes of the computer systems (technology that is; hardware and software) within the total concept of business continuity. The Operational Business Continuity Plan, for which ICT Operations deals with operational problems and office / workplace disaster recovery. These plans will form part of a comprehensive Business Continuity Plan.

4. PURPOSE AND OBJECTIVES OF THE POLICY

The primary objective of this policy is to establish a comprehensive approach to disaster recovery that safeguards data integrity, ensures system availability, and supports business resilience. To have the capacity to resume operational effectiveness within a specified period of time after the onset of a disaster or other disrupting events. It addresses both natural and human-made disasters, including cyberattacks, hardware failures, and environmental events.

This policy seeks to outline the Disaster Recovery controls for departmental employees to ensure that the data and information is correctly and efficiently backed up (stored) and recovered in line with best practice.

Furthermore, the policy seeks to ensure that the department conforms to a standard backup and recovery control processes in such a way that it achieves a balance between ensuring legislative compliance, best practice controls, service delivery efficiency. In addition, it seeks to define controls to enforce regular backups and support activities; so that any risks associated to the management of data backups and recovery are mitigated.

5. APPLICATION OF THIS POLICY

This policy applies to all employees (including service providers, contractors and temporary employees) utilising departmental systems and all or any aspect of COGTA networks.

6. SCOPE

This ICT Disaster Recovery Policy has been created to guide and assist the department to align with internationally recognised best practices, regarding data backup, recovery controls and procedures. This policy recognizes that government institutions are diverse in nature, and therefore each adopts the approach of establishing and clarifying principles and practices to support and sustain the effective control of data backup and recovery.

The policy applies to everyone in the department, including its service providers and consultants. This policy is regarded as crucial to the effective protection of data and information, of ICT systems of the department. Departments must develop its own Disaster Recovery controls and procedures by adopting the principles and practices put forward in this policy.

A disaster is an event that adversely impacts on COGTA's ability to process, provide, or utilize information essential to its day-to-day operations, or which causes an inability within COGTA to provide customers with basic services. The term disaster includes a failure or loss (whole or partial) of equipment and/or software and/or systems (including human resources) from whatever cause including but not limited to equipment failure, industrial actions, illness, configuration, explosion, earthquake, tornado, flood, subsidence, collapse, riot, contamination by smoke, water, chemicals or otherwise.

ul

7. LEGISLATIVE FRAMEWORK

The policy was developed with the legislative environment in mind, as well as to leverage internationally recognised ICT standards.

The following legislation, among others, were considered in the drafting of this policy:

- Constitution of the Republic of South Africa 1996.
- Copyright Act, 1978 (Act No. 98 of 1978)
- Electronic Communications and Transactions Act,2002 (Act No. 25 of 2002)
- Minimum Information Security Standards, as approved by Cabinet in 1996
- National Archives and Record Service of South Africa Act, 1996 (Act No. 43 of 1996)
- Promotion of Access to Information Act, 2000 (Act No. 2 of 2000) (PIAIA)
- Promotion of Administrative Justice Act, 2000 (Act No. 3 of 2000)(PAJA)
- Protection of Personal Information Act, 2013 (Act No. 4 of 2013) (POPI)
- Regulation of Interception of Communications Act, 2002 (Act No. 70 of 2002)
- Public Finance Management Act, 1999 (Act No. 1 of 1999)
- Public Service Act, 1994 (Proclamation No. 103 of 1994)
- Chapter 6 of Public Service Regulations, 2016

The following internationally recognised ICT standards were leveraged in the development of this policy:

- DPSA Information and Communication Technology Governance Policy Framework
- Control Objectives for Information Technology (COBIT) 5, 2012
- ISO 27002:2013 Information technology — Security techniques — Code of practice for information security controls
- King Code of Governance Principles, 2009

8. POLICY STATEMENTS

8.1 Policy Statement

All IT employees and other COGTA employees responsible for performing IT Continuity activities and procedures will follow the IT Recovery process as documented. The Department must have in place an approved Disaster Recovery Plan to ensure that it can recover all critical IT and information systems in the event of a disaster.

It is management's objective that all business units within COGTA have detailed IT Continuity Plans for their directorates 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.

The collection of individual business unit IT Continuity Plans will form the collective COGTA 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 Plan requirements are catered for and conform to the overall standard as prescribed by the IT Continuity Planning team.

The IT Continuity Plan must cover all essential, critical and regulatory business activities which relate to its daily operations. In the event of a disaster, it must be possible for the business unit affected and the Department to continue operating even at limited capacity in line with its service charter.

The IT Continuity Plan must 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 employees understands what is required for execution.

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

The employees must be made aware of the IT Continuity Plan and their specific roles (if applicable) defined within the plan.

8.2 Policy Ownership

The HOD remains Accountable for the overall ICT Disaster Recovery Policy. This responsibility is delegated to GICTM.

It is the responsibility of the business units (Branch, Chief Directorates, Directorates and units) to ensure that they have enough information in their specific section of the IT

Continuity Plan, to enable them to be recovered from an incident and continue to provide a service to clients within acceptable timeframes.

8.3 Policy Administration

The Director: GICTM is responsible for maintaining this policy. The ICT Steering Committee review the policy and changes. The Head of Department must approve the reviewed policy.

9. RESPONSIBILITIES OF ROLE PLAYERS

9.1 Directorates

In order to support the above policy statement fully, all directorates are expected to ensure that the following:

a) identify their critical business processes, functions and outputs
b) identify and assess any threats to those business processes, functions and outputs.
c) put in place measures to eliminate those threats, or if it is not possible, develop plans to mitigate and manage them, should they materialize.
d) comply fully with all the requirements of this IT Continuity Policy
e) Evaluate and recommend strategies for the reduction or transfer of risk
f) Develop the IT Continuity strategy consistent with the department overall business and security strategy.
g) Regularly test, review, and update all procedures relating to the IT Continuity Plan;
h) Ensure IT Continuity Planning is integrated into business functions and daily operations.
i) Allocate responsibility to individuals in their business units to fulfil the requirements of the IT Continuity plan.
j) Ensure that records are managed in accordance with the records management policy and that all the required IT Continuity documentation and records are available and current.

9.2 GOVERNMENT INFORMATION AND COMMUNICATION TECHNOLOGY MANAGEMENT

In by ensuring that the department's information and communication technology systems can be restored quickly and effectively after a disruption

a) GICTM shall be responsible for the development and maintaining of and where applicable the obtaining of approvals for the departmental Disaster Recovery Policy, Strategies, Plans and Procedures.

b) ensure that the Disaster Recovery Policy is implemented and reviewed on an annual basis.

c) Ensure that ICT Steering Committee report is submitted to the EMC for noting and ratification.

d) responsible for the distribution of this policy within the department and as such ensures that policy updates are effectively communicated. Where applicable, the GICTM should also monitor the implementation of this policy, plans and procedures to ensure the effective implementation hereof.

9.3 Third Party Vendors

With reference to areas where distributed processing takes place, each such third party and contractor within the department will be responsible for the implementation of, and overall compliance with Disaster Recovery Policy. These responsibilities will include identifying business needs, developing and testing of the plans to meet all requirements. This responsibility should be exercised with the assistance of the GITO and IT Steering Committee. It is vitally important that all externally provided systems and services (such as SITA and other IT service providers) be included in the disaster recovery plans, as these systems may fulfil a key function in the department. The external service provider should be included in the policy/ plans formulation and must adhere to the principals, strategies and procedures contained therein. An audit for compliance may have to be conducted to ensure that the plans and policies have been implemented.

10. KEY RISK AREAS

The key areas that can affect our delivery of service include, but are not limited to:

10.1 The denial of access to COGTA facilities due to, for example:-

a) Scene of crime investigation

b) Accidental fire or arson

c) Vandalism

d) Toyi-toyi (civil unrest)

e) Sabotage (arson, cyberattacks, hacking).

10.2 Employee shortages due to, for example:-

a) Loss of key employees/skills

b) Industrial action

c) Fuel shortage

d) Prolonged severe weather

e) A major pandemic outbreak

10.3 Denial of service due to for example:-

Failure of a supporting service such as:

a) IT Infrastructure fails

b) Computing system fails

c) A contractor's or service provider (internal and external) business fails

d) Communication and/or Telephone system fails

e) Unavailability of proprietary platform and critical information

10.4 Critical Systems Identification

a) Transversal systems (BAS, Persal, Logis) are hosted Nationally at SITA Head Office

b) Emails and Office 365 are cloud based hosted, and services will not be impacted as they do not require domain authentication.

11. RECOVERY STRATEGIES

11.1 Prevention and Mitigation

a) Cost effective prevention and mitigation measures must be investigated and applied.

b) Critical technology and information systems should be protected against potential hazards and threats by means of appropriate, practical and cost-effective measures of detection. This will reduce losses and lessen the impact of uncontrollable events.

c) The primary objective of detective and preventative control measures is to identify and implement feasible control measures to detect and prevent the occurrence of manmade and natural hazards, as well as to mitigate the effects of actual occurrences. Contingent controls are required to reduce the seriousness of risks, should they materialize.

11.2 Preparedness

a) An Operational Business Continuity Plan that addresses office/workplace recovery/critical business functionalities should be complied prior to a Disaster Recovery Plan. Disaster Recovery Plans form part of a comprehensive Business Continuity Plan.

b) Preparedness planning assures the identification of actions that need to be taken prior to and during disaster/emergency conditions. It will detail a plan of action, (who does what, when and where) and what resources are needed to respond to a given situation.

c) Planning must be based on a worst-case scenario and be flexible in order to cater for lesser events.

d) Depending on the recovery time frame required and the Disaster Recovery Strategy, extra computer, network and environmental equipment may need to be purchased, leased or shared, to enable a timely recovery.

e) All parties that must adhere to this policy are to ensure that accurate and thorough preparedness is planned.

11.3 Disaster Recovery Planning

a) All critical systems and technology platforms must have a disaster recovery plan developed and maintained. All defined disaster recovery plans must be reviewed and updated on an annually basis.

b) Disaster Recovery planning will result in documented plans for each computer system. These plans, in conjunction with tests, will ensure that no recovery actions are overlooked during the recovery and normalization processes. Secondly, should the regular employee who performs the recovery not be available, backup personnel (or vendor employee), identified in the DR Plan, must be able to perform the recovery and normalization. It is the responsibility of all identified personnel to ensure that they are fully aware of all details contained in their disaster recovery plan/s.

c) Disaster Recovery planning addresses the period immediately following the declaration of a disaster to the point where an acceptable level of computer system functionality is obtained with priority on critical business processes.

d) All Disaster Recovery plans are to be reviewed and updated at least once a year.

11.4 Testing

a) All disaster recovery plans must be tested on a regular basis to ensure currency, practicality and accuracy. At least one successful test must be conducted annually.

b) Test results must be reported to management and remedial actions planned and taken on any test anomaly.

11.5 Disaster Declaration

a) A disaster shall be declared when any event as listed in the definition of a disaster occurs. Or if an operational event occurs where the anticipated time required, substantially exceed/s the critical time frame as specified in the relevant disaster recovery plan, to rectify/restore unavailability of computer system/s. Responsibility for the declaration of a disaster lies with:

    i Physical Disaster Conditions with major business impacts the Head of Department is responsible for declaring a disaster that has a major business impact.

    ii Logical and isolated incidents within the centralized environment (Servers), GITO is responsible for declaring disasters for isolated incidents within the centralized environment.

iii Logical and isolated incidents within decentralized environments (LANs and Desktops), GITO is responsible for declaring disasters for isolated incidents within the decentralized environments.

ul

11.6 Normalization

a) Once recovery at the alternate site has been completed in accordance with the Disaster Recovery plan, a project should be initiated to plan and execute the return of technology systems to the original site or new site. It is the responsibility of the GITO delegates to initiate the project as well as to ensure that the return to normal phase is included in the Business Continuity Plan.

12. DISASTER RECOVERY STANDARDS

12.1 Critical data, which is critical to the department must be defined by the department and must be backed up.

12.2 Disaster Recovery must be located at a location that is physically different from its original creation and usage location.

12.3 Disaster Recovery Testing must be done Bi-Annually

12.4 Procedures for Disaster Recovery implementation and the testing of the procedures must be documented. These procedures must include, as a minimum, for each type of data:

a) A definition of the specific test to be done
b) The type(s) of software to be used
c) The frequency and time of data backup for recovery purposes.
d) Responsibility for data backup.
e) The location site(s) for the Disaster Recovery solution.
f) The storage media to be used.
g) Any requirements concerning the data backup archives.
h) Transport modes; and
i) Disaster Recovery methods

13. DISASTER RECOVERY SELECTION

13.1 All data and software are essential to the continued operation of the department, as well as all data that must be maintained for legislative purposes, must be backed up.

13.2 All supporting material required to process the information must be backed up as well. This includes programs; control files, install files, and operating system software.

13.3 The application owner, together with the GITO will determine what information must be backed up, in what form, and how often.

14. BACKUP TYPES FOR DISASTER RECOVERY

14.1 Full backups should be run weekly preferably on weekends, along with daily machine replication. This will also aid in ensuring that data can be recovered and when necessary full machine recovery can be performed.

14.2 Differential/Incremental backups must be used for daily backups. This ensures that the backup time window is kept to a minimum during the week while allowing for maximum data protection.

14.3 Machine replication is the process of cloning a VM and copying it to a different location so that at any stage one can restore a crashed, failed, or problematic version of the VM. In the event of a restore the process is very easy to follow and depending on the size of the machine can be quick.

15. DISASTER RECOVERY SCHEDULE

15.1 Choosing the correct Disaster Recovery Schedule:

(a) Backup and Disaster recovery schedules must not interfere with day-to-day operations. This includes any end of day operations on the systems.

15.2 Frequency and time of Disaster Recovery testing:

(a) Disaster Recovery testing has to mimic a disaster event. This means for a controlled time period, day to day operations will be disrupted during testing.

15.3 Previous Test Results:

(a) Previous testing results will be kept for documentation and tracking purposes.

16. DISASTER RECOVERY OBJECTIVES

16.1 Overall Disaster recovery Budgetary Objectives

As a guideline the total of capital and operating Disaster Recovery budgets, in respect of servers, clients and LAN facilities and applications should be restricted to less than 20% of the departmental IT Operational Budget. This includes operational backup as well as disaster Recovery measures.

Although no limit is prescribed, the capital and operating budgets in respect of decentralised environments should be reasonable, justifiable, and cost effective in

ll

comparison with the prevention and mitigation of potential business risks that could be attributed to a dependency on technology.

16.2 Client / Server Objectives

a) To reduce complexity and administration workload of Disaster Recovery Procedures to the maximum allowed by means of automation.

b) To reduce recovery time of primary server's backup facilities in the department, and all server related applications.

c) To limit the recovery time of centralized server backup facilities, to the actual critical time frame of the Department.

d) Where applicable, to reduce recovery time of secondary backup facilities.

e) For disaster recovery and operational recovery to become integrated to reduce cost and workload.

f) Disaster Recovery testing to be simplified to the point where regular testing (by means of disaster recovery systems and infrastructure) results in minimum impact to service, i.e. becomes transparent to daily service.

g) Perform an analysis on the impact that the loss of the server would have on LAN environments.

16.3 Network Objectives

Disaster recovery resilience to be fully implemented within the departmental network infrastructure.

16.4 LAN Objectives

a) To implement a backup strategy for all critical data hosted on production LAN's, as well as the off-site cycling.

b) To have effective Disaster Recovery Plans and backup facilities that have been tested, for all high priority Business Units.

c) To limit the recovery time at backup facilities, to the actual critical time frames for all high priority Business Units.

d) To establish a common Disaster Recovery facility for high priority Business Units and a common testing site for low, medium, and high priority business units.

17. BREACH OF POLICY

Any failure to comply with the rules and standards set out herein will be regarded as misconduct and/or breach of contract. All misconduct and/or breach of contract will be assessed by the department and evaluated on its level of severity. Appropriate disciplinary action or punitive recourse will be instituted against any employee or service provider, who contravenes this policy. Actions include, but are not limited to:

a) Revocation of access to departmental systems and ICT services;

b) Disciplinary action in accordance with the Public Service Act; or

c) Civil or criminal penalties e.g. violations of the Copyright Act, 1978 (Act No. 98 of 1978).

d) Punitive recourse against a service provider.

18. MONITORING AND EVALUATION OF THE IMPLEMENTATION OF THE POLICY

GICTM will report any challenges that arises in the implementation of this policy to the ICT Steering Committee.

19. COMMUNICATION / EDUCATION OF THE POLICY

The policy will be communicated throughout the department to all its employees using workshops, intranet and workgroups.

20. DISPUTE RESOLUTION MECHANISM

In the event of disputes arising out of this policy, such disputes will be dealt with in terms of the grievance procedure and labour legislation applicable in the Public Service.

21. APPROVAL OF THE POLICY

The policy will be approved by Member of Executive Council (MEC) on the recommendation of the Head of Department.

22. COMMENCEMENT DATE

The commencement date of this policy will be on the date of its approval.

23. REVIEW OF THE POLICY

This policy will be reviewed every five years from the approval date and/or when there are changes in legislation or the operating environment. However, where it is deemed not necessary to review the policy, evidence of the process leading to such a decision should be provided. This policy will remain in force until and unless it has been withdrawn and amended by the MEC.

24. VERSION CONTROL AND CHANGE HISTORY

Version Control	Date Effective	Approved By	Amendment
Start from	YYMMDD (effective date)	Contact person – full name & title.	Include any superseded procedures and what the amendment is to the document.
2025		MEC: Honourable Zolile Williams of Cooperative Governance and Traditional Affairs	

Table 3 - Version Control and Change History