Province of the
EASTERN CAPE
SOCIAL DEVELOPMENT

ICT CONTINUITY POLICY

Department of Social Development

Policy Registration 2026-05

TABLE OF CONTENTS

1. TERMS AND DEFINITIONS

Term	Definition
Access	The authorised capability to log into, interact with, or utilise the Department's technological platforms, data sets, networks, and physical Information and Communications Technology (ICT) facilities.
Business Impact Analysis	A systematic, analytical process deployed to determine and evaluate the potential operational, financial, and regulatory effects of an interruption to critical business functions resulting from a disruptive event or disaster.
Configuration	The specific operational and functional setup of a computer system, hardware component, network device, or software application, tailored to meet distinct departmental requirements.
Critical IT Systems	Information Technology applications and infrastructure whose failure or protracted downtime poses an immediate threat to the execution of statutory mandates, public welfare, or the institutional existence of the Department.
Disaster (ICT)	Any unplanned event (including, but not limited to, extreme weather conditions, systemic utility failures, or malicious acts of sabotage) that causes a catastrophic disruption or total failure of the Department's IT systems.
Disaster (Legislative Definition)	As defined by the Disaster Management Act No. 57 of 2002 (South Africa), a progressive or sudden, widespread or localised, natural or human-caused occurrence that causes or threatens to cause death, injury, or disease; damage to property, infrastructure, or the environment; or significant disruption of the life of a community.
Executive Management	The highest tier of administrative leadership within the Department — including the Accounting Officer (Head of Department), Deputy Directors-General, Chief Directors, and Senior Management Service (SMS) officials — responsible for defining strategic direction, managing systemic risks, and exercising executive oversight.
Head of Department	The appointed administrative head and Accounting Officer of the Eastern Cape Department of Social Development, vested with the primary operational and financial accountability for the department.
ICT Asset	Any tangible component (such as laptops, mobile devices, servers, and network routers) or intangible asset (such as software licences and systemic data packages) within the departmental infrastructure that holds institutional value and is managed throughout its operational lifecycle.

Incident	Any unplanned event or operational anomaly that disrupts, compromises, or reduces the delivered quality of an active ICT service.
Information Assets	Identifiable data resources, repositories, and knowledge management channels — encompassing physical paper records, digital client databases, operational software, and intellectual property — that are essential for departmental decision-making and statutory continuity.
Key Resources	The designated human capital, personnel, and specialised personnel formally appointed to execute critical recovery operations within the structures of the Disaster Recovery Plan (DRP).
Member of the Executive Council	The political head appointed by the Premier to oversee the social development portfolio within the province, providing executive governance and legislative alignment to the Department.
Risk	The formal product of the probability of a specific threat event occurring and the severity of its corresponding socio-economic or operational consequences.

Acronyms	
BCT	Business Continuity Team
CIO	Chief Information Officer
CM	Configuration Management
CMT	Crisis Management Team
COBIT	Control Objectives for Information and Related Technology
DRP	Disaster Recovery Plan
ECDSD	Eastern Cape Department of Social Development
ICT	Information and Communication Technology
IMT	Information Management Team
ISM	Information Security Manager
IT	Information Technology
ITIL	Information Technology Infrastructure Library
ITRT	Information Technology Recovery Team
MISS	Minimum Information Security Standard
SLA	Service Level Agreement

2. LEGISLATIVE FRAMEWORK

a) Constitution of the Republic of South Africa, 1996
b) National Strategic Intelligence Act, 1994 (Act No. 39 of 1994) *(As amended by the General Intelligence Laws Amendment Act, 2024)*
c) State Information Technology Agency Act, 1998 (Act No. 88 of 1998)
d) Public Finance Management Act, 1999 (Act No. 1 of 1999)
e) Promotion of Access to Information Act, 2000 (Act No. 2 of 2000)
f) Promotion of Administrative Justice Act, 2000 (Act No. 3 of 2000)
g) Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002)
h) Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act No. 70 of 2002)
i) Disaster Management Act, 2002 (Act No. 57 of 2002)
j) Protection of Personal Information Act, 2013 (Act No. 4 of 2013)
k) Cybercrimes Act, 2020 (Act No. 19 of 2020)
l) Minimum Information Security Standards (MISS, 1996)
m) SANS/ISO/IEC 27001:2022 (Information Security, Cybersecurity and Privacy Protection)
n) Control Objectives for Information and Related Technology (COBIT 2019)
o) Department of Social Development CIO Charter
p) Departmental ICT Business Continuity and Disaster Recovery Plan

3. PREAMBLE

This policy has been implemented since 2016. Upon the review process it has been discovered that most of the controls are still relevant. The Business Continuity Management is a continuous process of risk management ensuring the Department continues to deliver key services when disruption arises.

The Department shall provide contingency plans that aim at preventing and combating disasters. The contingency plans shall be geared for saving lives, safeguarding property and information, and ensuring work continues with minimal disruption. These measures shall be achieved through coordinated and effective preventive control measures of the contingency plan. This policy document provides an overall policy that governs the nature and detail to which Disaster Recovery is deployed and used within the Department.

4. PURPOSE

The purpose of this policy is to ensure departmental capacity to resume ICT operational effectiveness in the event of disaster and disruption.

5. OBJECTIVES

a) To ensure staff welfare and confidence during disaster incidents.
b) To maintain departmental stakeholder and client confidence.
c) To minimise the impact of ICT disruptions caused by disaster incidents.

6. SCOPE OF APPLICABILITY

The scope of this policy is applicable to all employees, contract workers and individuals granted access to departmental systems.

7. PRINCIPLES AND VALUES

a) **Confidentiality:** The Department's employees shall be ethical and maintain the legal obligation to protect sensitive information.
b) **Integrity:** The Department's employees shall practise honesty, consistency and ethical conduct.
c) **Availability:** The Department shall ensure systems and resources remain accessible.
d) **Accountability:** The Department shall ensure employees take responsibility for actions and outcomes.

8. POLICY PROVISIONS

a) ICT staff responsible for performing ICT continuity activities and procedures shall follow a single ICT Recovery process.

b) The Department shall have an approved comprehensive ICT Continuity Plan in place for ensuring recovery of critical ICT and information systems in the event of a disaster.
c) Business units shall have detailed continuity plans to ensure critical processes can be continued during unplanned disruptive events.
d) Business unit continuity plans shall inform the Department's DRP.
e) The DRP shall be periodically tested at pre-determined dates or on *ad hoc* basis to ensure implementability in emergency situations.
f) The disaster recovery plan shall cover all essential and critical business activities.
g) The DRP shall be kept up to date.
h) Users shall be made aware of the disaster recovery plan and their specific roles.
i) A multidisciplinary team shall be assembled to develop and review the Disaster Recovery Plan.
j) Business units shall ensure employees comply with the requirements of the Disaster Recovery Plan.
k) A Management Team shall be established:
When an incident of wide-ranging impact requires department-wide response.

8.1. When active, the CMT shall:

a) Take responsibility for coordinating active Information Technology Recovery Team / Business Continuity Team and for all communication with all external stakeholders, especially customers, suppliers, regulators, the media and the public.
b) Be responsible for declaring a disaster and activate the relevant disaster team.
c) Provide overall leadership role during disaster recovery process.

8.2. Declaration of Disaster

Declaration of the disaster shall only be made by the Head of Department.

9. APPROVING AUTHORITY

The Member of the Executive Council has the responsibility to approve the ICT Continuity Policy.

10. ACCOUNTABILITIES AND RESPONSIBILITIES

10.1. Application Owner

The owner of the information resource shall ensure contingency plans are developed to recover services after a disaster.

10.2. The Information Security Manager

Shall ensure security is considered in line with ICT Continuity Policy.

10.3. The Information and Communication Technology Unit

a) ICT shall remain responsible for the Disaster Recovery Plan.
b) ICT shall be responsible for ensuring business units have enough information in their specific section of the Continuity Plan.

10.4. The Head of Department

The Head of Department working in conjunction with the CIO shall be responsible to ensure effective implementation and compliance of this policy.

10.5. The Member of Executive Council

The Member of the Executive Council shall be responsible for the approval of this policy.

11. EFFECTIVE DATE OF THE POLICY

This policy shall be implemented from its effective date approval.

12. MONITORING MECHANISMS

The CIO and senior management shall be required to ensure ICT Operational Committee, ICT Steering Committee and Risk Committee exists to monitor and measure compliance with this policy.

13. REVIEW OF THE POLICY

The policy shall be reviewed after three years (3) and whenever there are new developments or legislation change.

14. ENFORCEMENT

a) Failure to comply with this policy shall result in disciplinary action in accordance with the Disciplinary Code and Procedures for the Public Service.
b) Any conduct that interferes with the normal and proper operation of the department's ICT systems, shall constitute a violation of the approved ICT Continuity Policy.
c) The Department executive management reserves the right to revoke the privileges of users.

15. POLICY RECOMMENDATIONS AND APPROVAL

RECOMMENDED/NOT RECOMMENDED

MR M. MACHEMBA
HEAD OF DEPARTMENT
EASTERN CAPE DEPARTMENT OF SOCIAL DEVELOPMENT
DATE: 08/06/2026

APPROVED/NOT APPROVED

MISS B. FANTA
MEMBER OF THE EXECUTIVE COUNCIL
EASTERN CAPE DEPARTMENT OF SOCIAL DEVELOPMENT
DATE: 17/06/2026

ANNEXURE A: ICT CONTINUITY MANAGEMENT PROCESS

A.1 Four stages of ICT Continuity management process

The disaster recovery management process will consist of the following four stages:

a) Stage 1: Planning
b) Stage 2: Implementation and Operation of DR Strategy
c) Stage 3: Monitor and Review
d) Stage 4: Maintenance and Improvement

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

B.1.1 Stage 1: Planning

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

B.1.2 Stage 2: Implementation and operation of ICT Continuity strategy

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

a) how effectively ECDSD will respond to and recover from an IT interruption or disaster;
b) any costs that will be incurred as a result of a business interruption or disaster;
c) requirements identified through the Business Impact Analysis and Risk Assessment activities; and
d) the outputs from the above activities that will feed into the disaster recovery strategy, which proposes risk reduction measures and recovery options, in support of business continuity.

Once the DR strategy has been agreed, the disaster recovery management lifecycle shall move into the actual implementation activities. These activities include:

a) establishing an ICT Continuity Plan with clear roles and responsibilities for any personnel who will be involved in a recovery;
b) developing training, awareness and competency plans;
c) developing implementation and supporting plans;
d) developing and implementing an incident response structure;
e) procuring recovery facilities;
f) validating continuity capability through initial testing;
g) embedding ICT continuity in the ECDSD culture;
h) developing and implementing change management procedures;
i) testing of the ICT continuity plan; and

j) disaster recovery documentation and records management.

B.1.3 Stage 3: Monitor and review

The completion of the first two stages of the business continuity management process will mean that a disaster recovery management solution has been analysed, agreed and implemented within the Department.
The ECDSD will then need to ensure that the strategy and recovery facilities are maintained as part of day-to-day business activities.
The CIO has responsibility for maintaining the disaster recovery management environment through a series of operational management activities.
These activities will include:

a) **Internal and external reviews** – each business unit shall be responsible for reviewing their own IT Continuity activities at agreed time intervals. The management committee shall ensure that the ICT Continuity Plan is tested on either an *ad hoc* basis or at planned intervals.

b) **Management reviews of the disaster recovery plan** – The test results from above will feed into the management review of the ICT Continuity Plan. The decisions and actions recommended by management will feed into the Maintenance and Improvement stage.

B.1.4 Stage 4: Maintenance and improvement

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

ECDSD shall document all procedures for corrective and preventative action to ensure that the ECDSD Disaster recovery Plan conforms to the PAS77 and BS25999 standard. All such procedures, minutes, records pertaining to DRP shall form part of the ECDSD disaster recovery records and documentation as required by the PAS77 and BS25999 standard.

ANNEXURE B: ICT CONTINUITY TESTING PROCEDURE

1.1 Exercising and Testing Methods

IT will ensure that one of the following testing methods is performed and the guidelines adhered to

1.1.1 Structured Walk-Through Testing:

1. The Incident Management Team will meet to verbally walk through the specific steps of each component of the disaster recovery process as documented in the disaster recovery Test plan.
2. Confirm the effectiveness of the plan and identify gaps, bottlenecks or other weaknesses in the plan.

1.1.2 Checklist Testing:

- Ensure telephone number listings are current and correct
- Copy of the recovery plan and operational manuals are available
- Review the plan and identify key components that should be current and available
- The checklist must ensure that IT complies with the requirements of the disaster recovery procedures.
- A combination of the checklist test and the structured walk-through test will be utilised for initial testing to determine modifications to the plan before attempting more extensive testing.

1.1.3 Simulation Testing

- IT will simulate a disaster so normal operations will not be interrupted.
- A disaster scenario should take into account the purpose of the test, objectives, type of test, timing, scheduling, duration, test participants, assignments, constraints, assumptions, and test steps into consideration.
- Include the notification procedures, temporary operating procedures, and backup and recovery operations while testing.
- Test the following elements during simulation: hardware, software, personnel, data and voice communications, procedures, supplies and forms, documentation, transportation, utilities (power, air conditioning, heating, ventilation), and alternative site processing. It may not be practical or economically feasible to perform certain tasks during a simulated test (e.g., extensive travel, moving equipment, eliminating voice or data communication).

1.1.4 Parallel Testing

- Perform a parallel test in conjunction with the checklist test or simulation test.

- Under this scenario, historical transactions, such as yesterday's transactions, are processed against the preceding day's backup files at the alternative Pretoria backup site.
- All reports produced at the alternate site for the current business date should agree with those reports produced at the existing processing site.

1.1.5 Full-interruption Testing

- This test could disrupt normal operations; therefore, it should be approached with caution and only tested after hours. A full-interruption test activates the total disaster recovery procedure.
- Ensure that adequate time is scheduled for the testing.
- The test should not be scheduled at critical points in the normal processing cycle, such as the end of the month.
- Predetermine the duration of the test in order to measure adequate response time.
- Ensure that various test scenarios are planned to identify the type of disaster, the extent of damage, recovery capability, staffing and equipment availability, backup resource availability, and time/duration of the test.
- Eastern Cape Department of Social Development (ECDSD) must announce exercising and testing.
- Scenario upon which the testing and exercising will be based: Assume the Head office is inaccessible; the IT services are down.
- Testing process: ECDSD will follow the disaster recovery procedure, in place to conduct their live and Offline Disaster Recovery test.

2 ECDSD Role on the ICT Continuity Test

The ECDSD IT department has a role to play on the ICT Continuity test. The ICT Continuity test is divided into two phases can either be online or offline test. The department can conduct both tests, but there are steps to follow prior to the tests;

Online ICT Continuity test;

1. Schedule a downtime and inform users prior to the DR test.
2. Provide list of servers to be tested.
3. Provide a technician/System admin with admin login details.
4. Provide technician who will conduct a detailed test to verify whether the DR test was successful, by log into servers at the DR site. The IT department will determine the measure to qualify whether the DR test was successful.
5. Ensure all critical ECDSD staff are available during the scheduled test.

NOTE: any changes made by ECDSD users while an online or live DR test is conducted will be lost hence it's critical that to schedule down time.

Offline ICT Continuity test;

1. Provide list of servers to be tested.
2. Provide a technician/System admin with admin login details.

Provide technician who will conduct a detailed test to verify whether the ICT Continuity test was successful, by login into servers. The department will determine the measure to qualify whether the DR test was successful.