Province of the
EASTERN CAPE
SOCIAL DEVELOPMENT

Backup and Retention Policy

Department of Social Development

Policy Registration 2026-02

TABLE OF CONTENTS

TERMS AND DEFINITIONS

Terms	Definitions
Access	The ability or permission to use, enter, or communicate with a system or physical environment.
Application Owner	The individual responsible for managing the technical and operational aspects of a specific application.
Archive	A physical or logical subnetwork that exposes an organisation's external-facing services to a larger and untrusted network, usually the internet.
Backup	The process of copying active files from online disk storage to secondary storage so that data may be restored in the event of damage or loss.
Backup Administrator	A person designated to perform the administration, functions, and maintenance of the backup solution.
End-User	An official or authorised individual who utilises the information, computer equipment, and systems of the Department to perform their duties.
Exchange Servers	A powerful email, calendar, and contacts solution that facilitates secure and efficient internal and external communication, primarily aimed at businesses and enterprise-level organisations.
Executive Management	The highest level of leadership (e.g., CEO, CFO, COO) responsible for defining organisational strategy, setting long-term goals, and making high-stakes institutional decisions.
File Server	A computer responsible for the storage and management of data files so that other computers on the same network can access them. It enables users to share information over a network without having to physically transfer files.
Grandfather-Father-Son (GFS)	A data retention strategy involving the maintenance of backups from different periods: weekly, monthly, and yearly.
Head of department	The Accounting Officer of the Eastern Cape Department of Social Development, as defined by the Public Finance Management Act.
ICT Asset	Any tangible or intangible component within the Department's IT infrastructure that adds value and holds data. Examples include hardware (laptops, servers), software licences, network components, and data, all of which are tracked, managed, and maintained throughout their lifecycle.
ICT Continuity Plan	A comprehensive set of procedures on how to respond to a disruption or incident, how to protect critical information and assets, and how to restore operations and services as quickly as possible.
IT Disaster Team	A disaster recovery team consisting of a group of individuals focused on planning and implementing an ICT Continuity Plan.
LAN Data Server	A computer within a Local Area Network (LAN) specifically designated to provide shared resources, services, or applications to other devices on the same network, facilitating efficient communication and resource sharing.
Member of the Executive the Council	The Executive Authority appointed by the Premier to provide political leadership and oversight to the Provincial Department.
Replication	The process of making a replica (a copy) of data to an offsite disk storage.
Repository	A storage location used to store backups of data and systems.
Acronyms	
CFO	Chief Financial Officer

CIO	Chief Information Officer
ECDSD	Eastern Cape Department of Social Development
GITO	Government Information Technology Officer
HOD	Head of Department
ICT	Information and Communication Technology
ISS/RM	Information System Security/ Risk Management
IT	Information Technology
RPO	Recovery Point Objective
RTO	Recovery Time Objective

LEGISLATIVE FRAMEWORKS

1. Constitution of the Republic of South Africa, 1996
2. Public Finance Management Act, 1999 (Act No. 1 of 1999)
3. Promotion of Access to Information Act, 2000 (Act No. 2 of 2000)
4. Promotion of Administrative Justice Act, 2000 (Act No. 3 of 2000)
5. Private Security Industry Regulation Act, 2001 (Act No. 56 of 2001)
6. Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002)
7. Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act No. 70 of 2002)
8. Protection of Personal Information Act, 2013 (Act No. 4 of 2013)
9. State Information Technology Agency Act, 1998 (Act No. 88 of 1998)
10. National Archives and Records Service of South Africa Act, 1996 (Act No. 43 of 1996)
11. Protection of Information Act, 1982 (Act No. 84 of 1982)
12. Public Service Regulations, 2016
13. Minimum Information Security Standards (MISS), 1996
14. Guidelines for the Handling of Classified Information (SP/2/8/1), 1988
15. National Cloud Computing Legislation Principles: Guidance for Public Sector Authorities Moving to the Cloud, 2015
16. ICT Continuity Plan, 2016
17. SABS/ISO 17799:2005: Information Technology – Security Techniques – Code of Practice for Information Security Management.
18. ISO/IEC 27001: Information Security Management Systems (ISMS) – Requirements.
19. ISO/IEC 27002: Code of Practice for Information Security Controls.

3. PREAMBLE

This policy is formulated in accordance with the legislative frameworks and standards issued by National Intelligence regarding **Minimum Information Security Standards (MISS)**. The primary objective of this document is to ensure that control objectives are strengthened and that departmental information assets are rigorously secured, monitored, and managed.

The Department acknowledges the critical importance of computing resources and remains committed to the continuous support and enhancement of information systems security.

The rapid development and progression of information technology and complex system networks have escalated threats to information systems security. This evolution necessitates the establishment of robust information management policies, stringent standards, and comprehensive control measures to protect the Department's information assets against emerging security risks.

This policy provides a systematic and standardised approach to data management. Its purpose is to ensure that all departmental data is adequately protected and remains fully recoverable in the event of data loss, technical failure, or operational disruptions. Through the implementation of these controls, the Department maintains the **availability, confidentiality, and integrity** of its digital environment.

4. PURPOSE

The purpose of this policy is to provide guidance ICT continuity and data back administration processes with the aim of minimising the business impact and disruption of ICT services and business services.

5. OBJECTIVES

To be able to restore business data and ICT services with no loss or with minimal loss.

6. SCOPE OF APPLICABILITY

This policy is applicable to all employees, contract workers and individuals granted access to departmental systems.

7. PRINCIPLES AND VALUES

a) **Confidentiality:** The Departmental employees shall be ethical and maintain the legal obligation to protect sensitive information.
b) **Integrity:** Employees shall practise honesty, consistency and be ethically firm.

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

Controls shall be established to ensure proper management of risks associated with ownership and safeguarding of information which shall include:

a) Implementing and enforcing storage of department approved information on computers and servers, to ensure that data such as audio-visual files do not take up space on the storage facilities.

b) Enforcing centralised storage of documents on LAN Data servers (preferably with offline folder synchronisation for mobile laptops) to facilitate centralised data backup.

c) Ensuring that critical system generated data stored on the servers is backed up.

d) Ensuring that data is replicated to an off-site location in case of a disaster.

e) Advanced scheduling, automated unattended operation, centralised reporting, and enterprise-wide media management.

f) High-performance backup and restoration features that reduce the backup and restoration window.

g) The CIO Branch ensuring backup procedures adhere to international standards and procedures.

h) The CIO Branch ensuring that in the event of disaster, backup files can be recovered by:

   i) Implementing scheduled unattended but auditable backup systems.

   ii) Implementing a backup solution that minimises the data recovery time.

   iii) Implementing a disaster recovery solution that achieves the Recovery Time Objective. (RTO) and Recovery Point Objectives.

i) The CIO Branch ensuring data integrity by regularly testing the restorability of backup data monthly.

j) The CIO Branch enabling the recoverability of information by ensuring that offsite storage facilities are maintained regularly.

k) The ICT Unit upon receipt of an authorised request from the Head of Department or delegated authority, retrieving and providing relevant electronic information required.

l) Performing ICT Continuity testing twice a year and Backup Restore tests quarterly.

m) Authorisation obtained from the Head of Department prior to effecting any changes on the backup procedures and the IT Continuity Plan.

8.1. Server Based Data

a) Data servers and systems shall be regularly backed up, safeguarding it against accidental deletion, hardware failures, data corruption, and cyberattacks.

b) The department's minimum and maximum retention periods of information shall be based on contractual, legislative and industry requirements.

c) All backups containing sensitive data shall be encrypted.

8.2. Replication

a) All business-critical systems shall be replicated to an off-site backup storage within the SITA data centres.

b) All replicated offsite backups containing sensitive data shall be encrypted while in transit and at rest.

c) In the event of onsite backup storage being offline and damaged, reliable backup copies shall enable the Department to quickly recover its operations, minimising downtime, data loss and mitigating the impact on business processes.

d) All archival backup data stored off-site shall be reflected in an up-to-date directory that shows the most recent date on which the information was modified and the nature of the information.

8.3. Backup Infrastructure

a) ICT shall manage the storage space for backups, ensuring adequate capacity and regular purging of outdated backups. Consulting Records Management and Archive Policy

b) All storage devices on which sensitive, valuable or critical information is stored for periods longer than six months shall not be subject to rapid degradation. Such media shall be tested at least annually to ensure that information is still recoverable.

8.4. Backup Types

The Department shall put the following mechanisms in place:

a) Incremental backups performed daily followed by other scheduled backups.

b) All full backups will be replicated to the offsite location.

8.5. Backup Testing

The Department shall put the following mechanisms in place:

a) Testing of backup copies performed to ensure integrity and successful data restoration.

b) Testing of replicated backup copies performed to ensure integrity and successful data restoration.

c) Testing of Cloud workload backups performed to ensure integrity and successful data restoration.

8.6. Data Retention and Disposal

The Department shall ensure the protection of electronic records against alteration or deletion. The following shall apply:

a) Data backups shall be appraised by the Records Management.
b) Data and Data backups shall be retained for a period stipulated by fully established Records Management Forum in line with legislations.
c) Records Management shall apply for records appraisal and disposal authority for data backups before deletion or transfer to archival custody.

9. APPROVING AUTHORITY

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

10. ACCOUNTABILITIES AND RESPOSIBILITIES

10. 1. The Chief Information Officer

a) The CIO shall be responsible for the implementation of this policy and ensure that directives are effectively executed.
b) Shall lead the ICT disaster recovery team and perform the necessary duties as specified in the ICT Continuity Plan.
c) Shall ensure that mechanisms to monitor and measure compliance exist with this policy.

10. 2. Application Owner

a) The designated owner of the information asset shall take responsibility for access granted to the officials.
b) The application owner of the information resource shall ensure that access to the resource granted is appropriate and justified in accordance with the information classification.

10. 3. The Director ICT Engineering

a) Shall be responsible for ensuring that the ICT continuity testing report is recommended and approved by the Head of Department.
b) Shall form part of the ICT disaster recovery team and perform the necessary duties as specified in the ICT continuity plan.

10. 4. The Deputy Director: ICT Infrastructure

a) Shall ensure that any network and server related issues are resolved for the smooth running of backup processes.

b) Shall be responsible for coordinating the daily backups, monitoring and reporting.
c) Shall ensure that any backup failures and errors are timeously resolved.
d) Shall be responsible for ensuring full functionality of ICT continuity equipment.
e) Shall ensure that backup restore tests are performed and escalated.
f) Shall facilitate the review and resolution of backup failures and errors.
g) Shall store the replication disk backup in a safe and secure offsite location.
h) Shall be responsible to ensure full functionality of the data centres, LAN and WAN.
i) Shall ensure that the testing of ICT continuity plan is performed to prevent data loss.
j) Shall be responsible for the maintenance of this policy.

10.5. Departmental Users

The Departmental Users shall store all work-related information on the OneDrive for business account.

10.6 Records Management Forum

The Records Management Forum is responsible for identifying all expired electronic documents hosted on the ICT LAN Server and notifying ICT to dispose of them in the system once their maturity is reached, in accordance with the approved disposal policy.

10.7 Member of the Executive Council

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

10.8 Head of Department

The Head of Department working in conjunction with the CIO shall be responsible for ensuring the effective implementation and compliance of this policy and standards procedures.

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 exist to monitor and measure compliance with this policy.

14. ENFORCEMENT

a) Failure to comply with this policy shall result in disciplinary action, in line with the Departmental code of conduct.

b) Any conduct that interferes with the normal and proper operation of the departments ICT systems, shall constitute violation of the approved Backup Policy.

c) The Department's Executive Management reserves the right to revoke the privileges of users.

13. REVIEW OF THE POLICY

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

15. POLICY RECOMMENDATION AND APPROVAL

Recommended/Not Recommended

MR. M. MACHEMBA
HEAD OF DEPARTMENT
EASTERN CAPE DEPARTMENT OF SOCIAL DEVELOPMENT
DATE: 04/05/2026

Approved/Not Approved:

MS. B. FANTA
MEMBER OF THE EXECUTIVE COUNCIL
EASTERN CAPE DEPARTMENT OF SOCIAL DEVELOPMENT
DATE: 04/05/2026