



Province of the
EASTERN CAPE
SOCIAL DEVELOPMENT

INFORMATION MANAGEMENT AND DATA GOVERNANCE POLICY

Department of Social Development

Policy Registration 2026-09

TABLE OF CONTENTS

Contents	Page
1. DEFINITIONS OF TERMS	3
2. LEGISLATIVE FRAMEWORKS	8
3. PREAMBLE.....	9
5. OBJECTIVES.....	9
6. SCOPE OF APPLICABILITY	9
7. PRINCIPLES AND VALUES	9
8. POLICY PROVISIONS	10
9. APPROVING AUTHORITY	13
10. ACCOUNTABILITIES AND RESPONSIBILITIES.....	13
11. EFFECTIVE DATE OF THE POLICY	18
14. POLICY REVIEW.....	19
15. POLICY RECOMMENDATIONS AND APPROVAL	19

DEFINITIONS OF TERMS

TERM	DEFINITION
Business	The business of ECDSD refers to ECDSD's service delivery and internal support activities.
Best Practices	Best practices are practices and processes that have been proven to be working well and produce good results.
Capturing	Refer to the process of transferring knowledge from one employee's mind into tangible resource such as text document.
Communities of Practice	Communities of Practice (CoP) are groups of people who organise themselves informally to develop competence and good practice in a specific domain.
Culture	Culture is a way of doing things. It includes values, norms, standards, processes and behaviours in a department or entire public service.
Corporate Public Service-wide level	A group of related departments that enables the Public Service to achieve its strategic mandate
Corporate Governance of ICT	The system by which the current and future use of ICT is directed and controlled. Corporate governance of ICT involves evaluating and directing the use of ICT to support the organization and monitoring this use to achieve plans. It includes the strategy and policies for using ICT within an organisation. (ISO/IEC 38500: 2008: 3)
Change Management	Collective term for all approaches to prepare, support, and help individuals, teams, and organisations in making organizational change. It includes preparing and supporting employees, establishing the necessary steps for change, and monitoring pre- and post-change activities to ensure successful implementation.
Data	Data is a set of elements gathered and stored for future use. These elements may include figures, pictures, images, statistics etc.
Data Classification	Refers to a process of organising data by relevant categories so that it may be used and protected more efficiently.
Data Governance	The exercise of authority, control, and shared decision-making (planning, monitoring, and enforcement) over the management of data asset.
Data Management	The development, execution, and supervision of plans, policies, programs, and practices that deliver, control, protect and enhance the value of data and information assets throughout their lifecycle (DAMA, 2017).

TERM	DEFINITION
Data Steward	An IT or business professional responsible for managing, protecting, and ensuring the quality, accuracy, and usability of an organization's data assets.
Data Owner	The official ultimately responsible for the data and information being collected and maintained by their Directorate, usually a member of senior management.
Data Custodian	Data Custodians are officials responsible for maintaining and backing up the systems, databases and servers that store ECDSD's data.
Data Creator	All employees of ECDSD can be data creators.
Data User	It is the individual official that interacts with, accesses, uses or updates data for the purpose of performing a task authorised by the data owner.
BI Dashboard	BI dashboard is a single-page Business Intelligent interactive that uses visualizations to highlight key metrics and data insights, curated from one or more underlying reports.
Department Level	A group of related components that enables a department to achieve its strategic mandate.
Evidence	Evidence is information or data used to support (or contradict) management decisions that inform policy development; programmatic interventions and to evaluate results of programme implementation.
Executive Management	The executive management is the higher body responsible for decision-making of ECDSD that consists of Accounting Officer, Deputy Director General, Chief Directors and SMS level.
Explicit Knowledge	Explicit knowledge is knowledge that has been articulated, codified, and stored in certain media. It can be readily transmitted to others.
Governance Champion	The Manager in ECDSD who is responsible to drive Corporate Governance of and Governance of ICT.
Governance Principles	The vehicle to translate the desired behaviour into practical guidance for day-to-day management (COBIT 5 Framework Exposure Draft: 29).
Head of Department	Head of Department for Eastern Cape Department of Social Development.
Members of Executive the Council	The Member of the Executive Council is the executing authority appointed by the Premier to lead the Provincial Department.

TERM	DEFINITION
4IR	4IR The 4th industrial revolution is a vision or visionary of the future involving further developments of information and communication technology, biotechnology, and an array of related developments. It is less about technology than change in human routines and practice in the use of technology.
Information	Information is data that has been analysed and processed to give it meaning within a particular context. Information is presented and visualised in different ways e.g., infographics to summarise findings from large data sets.
Information Management	It is an activity that includes collecting, collation, capturing, storing, retrieval and dissemination of information from external and internal resources.
Innovation	The process of transforming an idea, generally generated through research and development, into a new or improved product, process or approach which relates to the real needs of society.
Intellectual Property	Describes the application of the mind to develop something new or original.
Intellectual Capital	Refers to the potential value of intangible organisational components in a department that improve the value and application of the potential to the public service delivery.
Knowledge	Knowledge is a body of understanding and skills that is constructed by people through both formal learning and practical experience which enhances their decision-making capacity.
Knowledge Champion	Knowledge Champion is a facilitator of knowledge transfer through advocacy for knowledge sharing; support of KM initiatives at a high level and by linking colleagues to knowledge resources outside of their immediate context.
Knowledge Harvesting	It is the process of capturing and transferring the know-how in an expert's head into information assets that can be used to improve corporate performance and develop institutional memory.
Knowledge Management	Knowledge Management (KM) is a key organisational function, with processes and activities that involve collecting, collation, sharing, packaging, dissemination and use of knowledge in decision-making and enhancing organisational learning for improved service delivery with Departments.
Knowledge Management Strategy	Outlines plans, processes and actions which government desires to achieve regarding knowledge and knowledge management objectives. Knowledge management links the

TERM	DEFINITION
	government department's strategy with knowledge management activities. The strategy outlines how knowledge can support the achievement of the objectives set by government.
Knowledge Management System	Consists of KM culture, structure governance and leadership, roles and responsibilities, planning, technology, processes and operation.
Knowledge Sharing	It is the practical learning and takes place in workshops, during team discussion or anywhere where knowledge is shared.
Knowledge Transfer	Refers to the dissemination of knowledge from one party to the next party by various channels and taking place in different ways such as education, learning, sharing, storytelling, writing and publishing.
Knowledge Worker	Knowledge Workers are individuals whose work primarily focuses on the creation of knowledge at work. They are workers whose abilities include finding, synthesising, communicating, sharing, applying and packaging knowledge.
Learning Organisation	An organisation that tries to develop its human resources to their full potential and uses learning as a means of improving its business performance.
Public Service	Means all national departments; national government components listed in Part A of Schedule 3 to the Public Service Act; provincial departments which means the Office of a Premier listed in Schedule 2 to the Public Service Act; and provincial government components listed in Part B of Schedule 3 to the Public Service Act, and their employees.
Policy Framework	The Corporate Governance of ICT Policy Framework (CGICTPF).
Public Administration	Means the Public Service, municipalities and their employees.
Tacit Knowledge	Tacit knowledge (as opposed to formal, codified, or explicit knowledge) is the kind of knowledge that is difficult to transfer to another person by means of writing it down or verbalising it.
Data Management Maturity (DMM) Model	A comprehensive framework of data management.

ACRONYMS

BAS	Basic Accounting System
CIO	Chief Information Officer
CoP	Community of Practice
DPSA	Department of Public Service and Administration
ECDSD	Eastern Cape Department of Social Development
EDRMS	Electronic Documents and Records Management System
ICT	Information and Communication Technology

IM	Information Management
IP	Intellectual Property
ISO	Information Organisation for Standardization
IT	Information Technology
KM	Knowledge Management
KMSC	Knowledge Management Steering Committee
MEC	Member of the Executive Council
PARS	Provincial Archives and Records Service
PERSAL	Personnel and Salary System
RM	Records management
SDIMS	Social Development Information Management System
ICT	Information and Communications Technology, also referred to as IT
HOD	Head of Department or Organisational Component as per the PSA
GWEA	Government-wide Enterprise Architecture
SITA	State Information Technology Agency
AG	Auditor-General of South Africa
COBIT®	Control Objectives for Information Technology
CGICTPF	Corporate Governance of ICT Policy Framework
ISO/IEC 38500	International Standard on Corporate Governance of ICT (ISO/IEC WD 38500: 2008: 1)
PSA	Public Service Act 103 of 1994, as amended
DC	Data Champions
DAMA - DMBOK	Data Management Body of Knowledge

LEGISLATIVE FRAMEWORKS

1. Constitution of the Republic of South Africa, Act 108 of 1996
2. Public Finance Management Act, 1999 (Act No. 1 of 1999)
3. The Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002)
4. National Archives and Records Service of South Africa, 1996 (Act No. 43 of 1996)
5. Protection of Information Act, 1982 (Act No. 84 of 1982)
6. Promotion of Access to Information Act, 2000 (Act No. 2 of 2000)
7. Protection of Personal Information Act, 2013 (Act No. 4 of 2013)
8. Regulation of Interception of Communication Act, 2002 (Act No. 70 of 2002)
9. Spatial Data Infrastructure Act, 2003 (Act No. 54 of 2003)
10. State Information Technology Act, 1998 (Act No. 88 of 1998)
11. Labour Relations Act, 2002 (Act No. 12 of 2002)
12. The Public Service Act, 1994 (Proclamation No. 103 of 1994), (as amended)
13. The Public Service Act, 1994 (Act No. 108 of 1994)
14. Public Service Regulation (PSR 2008)
15. Public Service Regulations, 2016

POLICIES REGULATIONS

- a) Minimum Information Security Standard (MISS)
- b) Minimum Interoperability Standards (MIOS)
- c) National Development Plan (NDP) Vision 2030
- d) Disaster Recovery Policy (2016)

1. PREAMBLE

The ECDSD adopted the Data Management Body of Knowledge (DAMA – DMBOK) Framework to establish its enterprise-wide data management program critical to ECDSD meeting regulatory and business imperatives. Information is a corporate asset, important for ongoing operations and in providing evidence of business decisions, activities and transactions.

This Information and Data Management Policy sets out the commitment, direction and intent of strategic management pertaining to governance of the information and data management practice of ECDSD.

The policy commits the intention of data governance to ensure that data is reliable, consistent, complete, easily available to users, and unavailable unauthorised users. It outlines how ECDSD captures, stores, shares, and uses knowledge and information to achieve its objectives.

2. PURPOSE

The purpose of this policy is to provide successful data, information use and relevant input to management decision-making aligned to ECDSD's strategic and operational priorities.

3. OBJECTIVES

- a) To guide the identification of the information business.
- b) To source, categorise and store information and data.
- c) To manage the use of information, data and its transformation into information.
- d) To adopt a data governance framework.
- e) To comply with legislation.
- f) To ensure the right knowledge is available to employees.

4. SCOPE OF APPLICABILITY

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

5. PRINCIPLES AND VALUES

- a) **Confidentiality:** ECDSD 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:** ECDSD shall ensure systems and resources remain accessible.
- d) **Accountability:** Department shall ensure employees take responsibility for actions and outcomes.

6. POLICY PROVISIONS

6.1. Data Governance

A Data Governance framework, including standards and processes, shall be established to ensure that appropriate authority and control is applied to data in line with legislative and other compliance obligations.

6.1.1. Data Management

The data management process shall specify data collection, storage, access, use, disclosure, archiving and disposal to meet data quality, legislative and regulatory obligations.

6.1.2. Data Architecture

Data architecture shall address data in storage and data in motion with descriptions of data stores, data groups, data items and mappings of those data artefacts to data qualities, applications, and locations. Data shall be defined consistently, and the definitions are understandable and available to all users. In this context:

- a) Solution Architecture relates to higher level data entities, their relationships in line with a standardised model, as well as Data transfer objects and the defined boundaries of system and business integration points.
- b) Enterprise Architecture relates to Low Level Data Entities, their relationships, as well as Data Transfer Objects internal to the solution, and defined integration points for the solution.

6.1.3. Reference and Master Data

- a) ECDSD shall establish reference and master data management processes of defining how master data and reference data shall be created, integrated, maintained and used.
- b) The master data management process shall comprise of users, processes, and technology and shall link corporate critical data and provide a common point of reference and sharing to facilitate computing in multiple system architectures, platforms and applications.

6.1.4. Data Integration and Interoperability

- a) ECDSD shall establish data integration and interoperability processes relating to movement and consolidation of data.
- b) Integration shall consolidate data into consistent forms, either physical or virtual.
- c) Conceptual, logical and physical data models shall enable data integration between systems.
- d) Data owners shall ensure that data is fit-for-purpose and shall facilitate data integration.
- e) ECDSD shall maintain a shared library of data exchange standards.

6.1.5. Data Security

- a) ECDSD shall establish data security measures including protective digital privacy measures applied to prevent unauthorised access to computers.
- b) The data security process shall include the planning, development, and implementation of data related security policies, standards and procedures.
- c) All employees of ECDSD shall be responsible for appropriately respecting and protecting the data asset.
- d) Data shall be safeguarded to maintain the confidentiality and privacy of personal information.

6.1.6. Data Storage and Operations

- a) ECDSD shall establish data storage and operations processes which shall include the design, implementation, and support of stored data.
- b) Data and information shall be stored throughout its existence in an environment suited to its format and security classification.
- c) Information shall be stored in systems and according to classifications, frameworks and procedures to enable identification and retrieval.
- d) Information held in digital formats shall be managed and stored to ensure usability and accessibility.
- e) Business units and System/Data Owners shall be responsible for the storage of data in an environment that is secure.
- f) ECDSD shall adopt a consistent approach towards data server hosting including the use of a centrally managed and virtualised private 'cloud' solution.
- g) A disaster recovery plan shall be created, implemented and rehearsed to ensure service disruption is minimised.
- h) Database Administrators (DBAs) shall be involved in both aspects of data storage and operations as this is a highly technical side of data management.

6.1.7. Document and Content Management

- a) ECDSD shall establish document and content management processes to control the capture, storage, access and use of data and information.
- b) Focus shall be on maintaining the integrity and enabling access to documents and unstructured or semi-structured information equivalent to data operations management for relational databases.

6.1.8. Data Quality

- a) ECDSD shall establish data quality programs and standards to ensure its data is up-to-date, complete and of sufficient quality.
- b) Data quality criteria shall include the integrity, accuracy, completeness, timeliness, relevance, consistency and reliability of data.
- c) Quality metrics for departmental data shall be established, and a data quality profiling and cleansing plan shall be created.
- d) Data integrity shall be supported by roles, including data ownerships, stewardships, and custodianships of eligible users.
- e) Sharing information across departmental boundaries shall be facilitated.

- f) Data integration across ECDSO shall be encouraged to foster data accuracy and uniformity.

6.1.9. Warehousing and Business Intelligence

- a) ECDSO shall establish an enterprise data warehouse as a central repository of integrated data from disparate sources of current and historical data.
- b) The data warehouse shall support data virtualisation in ECDSO.

6.1.10. Data Management Maturity Assessment

- a) ECDSO shall establish a data management maturity program to assess the enterprise data management function.
- b) This function shall be sustained by business, and the program shall centre around the Data Management Maturity (DMM) model.

6.2. Data Classification

6.2.1. Data Classification Categories.

ECDSO data shall be classified into one of the following categories:

a) Public

Public data may be shared with a broad audience both within and outside ECDSO and no steps shall be taken to prevent its distribution.

b) Internal

Internal data shall not be disclosed outside of ECDSO without the permission of the person or group that created the data due to its potential sensitivity.

c) Confidential

Confidential data shall be sensitive data that if compromised could negatively impact operations, including harming ECDSO and its stakeholders.

d) Restricted Use/Top Secret

Restricted Use data shall include information that business unit has a contractual, legal, or regulatory obligation to safeguard stringently.

6.2.2. Data Classification System.

A data classification system organises data into categories based on its sensitivity, value, and regulatory needs. This policy shall implement three (3) types of data classification systems:

- a) **Manual** — This is a traditional data classification method which require human intervention and enforcement.
- b) **Automated** — Use of technology-driven solutions eliminate the risks of human intervention, including excessive time and errors, while adding persistence (around-the-clock classification of all data).
- c) **Hybrid** — Human intervention provides context for data classification, while tools enable efficiency and policy enforcement.

6.3. Knowledge Management

A knowledge management system shall be created which shall be used to coordinate the capturing, storing, processing, use of knowledge within ECDS.

6.3.1. Translate Individual and Organizational Learning into Organizational Intellectual Capital.

- a) Create a culture of learning organization through practices like coaching and mentoring.
- b) Develop a knowledge base for the Department.
- c) Communication Service Standard.

6.3.2. Capture and Preserve Organizational Intellectual Capital

- a) Develop the database and archiving system.
- b) Capture case studies and success stories.
- c) Sharing success and failures – story telling, brainstorming, exit interviews.

6.3.3. Develop Institutional Portal

- a) Implement Self Service Portal – e.g. Website and Intranet.
- b) Develop knowledge repository for frequently asked questions.
- c) Create search engine for information.
- d) Information access control and security to protect intellectual property.

7. APPROVING AUTHORITY

The Member of the Executive Council has the responsibility to approve the ICT Information Management and Data Governance Policy

8. ACCOUNTABILITIES AND RESPONSIBILITIES

8.1. Chief Data officer shall:

- a) Develop the business aligned data strategy, data architecture and data management strategy for the department.
- b) Ensure the approval of the department's data strategy, data architecture and data management strategy.
- c) Develop data management policies, standards, practices and procedures for the department.
- d) Lead the Data Management Maturity Assessment in the department.
- e) Establish and monitor adherence to metrics for all data management functions in the department.
- f) Champion the data management programme including communicating its importance to all the department's stakeholders.
- g) Ensure effective governance, storage, operations and analytics of data in the department.

- h) Collaborate with stakeholders to leverage data thus drive value for the department.

8.2. Data Governance Committee /delegated governance structure shall:

- a) Recommend the departmental data management programme including the data management strategy and data strategy for approval.
- b) Review and recommend the department's data architecture, policies, principles, standards and metrics for approval.
- c) Monitor compliance with legislative and regulatory requirements with regards to management of data in the department.
- d) Provide oversight into consistent and transparent use of data and information.
- e) Provide oversight to relevant data management sub-committees or working groups.
- f) Create internal alignment and communicate the data management programme in the department.
- g) Provide oversight into the management and resolution of data governance related issues.

8.3. The Data Stewards shall:

- a) Ensure data quality, integrity, implementation, and enforcement of data management within their area of work.
- b) Ensure data classification and approve access, under delegation from a Data Owner.

8.4. Data Warehousing Manager shall:

- a) Develop data warehouse policies informed by Data Management policy.
- b) Integrate internal and external data sets into ECDSD data warehouse.
- c) Monitor data integrity of the warehoused data.
- d) Develop data warehouse Standard Operating Procedures and process maps.
- e) Lead data warehousing projects.

8.5. Data Owner

The data owner shall:

- a) Review and categorise data and information collected.
- b) Assign data classification labels based on the data's potential impact.
- c) Ensure data compiled from multiple sources is classified with the most secure classification level.
- d) Ensure data shared between departments is consistently classified and protected.
- e) Ensure information with high and moderate impact level is secured in accordance with regulations.
- f) Develop data access guidelines for each data classification label.

8.6. Data Custodians

Data Custodian shall:

- a) Ensure that proper access controls are implemented, monitored and audited in accordance with the data classification labels assigned by the data owner.
- b) Submit an annual report to the data owners that addresses availability, integrity and confidentiality of classified data.
- c) Perform regular backups of internal departmental data, periodically validate data integrity and restore data from backup media.
- d) Fulfil the data requirements specified in ECDSD's security policies, standards and guidelines pertaining to information security and data protection.
- e) Monitor and record data activity, including information on who accessed what data.
- f) Encrypt sensitive data at rest while in storage; audit storage area network (SAN) administrator activity and review access logs regularly.
- g) Ensure that information with high and moderate impact level is secured in accordance with state regulations and guidelines.

8.7. Data User

The Data User shall:

- a) Use data in a manner consistent with the purpose intended and comply with the Information Management and Data Governance Policy.
- b) Have authorisation to handle and use the data and provide feedback or answer questions about the data classification tags.

8.8. Data Champion

- a) Shall be responsible for the organisation's use of data for business purposes.
- b) Shall ensure that data is protected and used appropriately.
- c) Shall be responsible for data strategy, including quality, governance, and data modernisation.
- d) Shall make sure business stakeholder will support and drive data classification efforts as a part of the ECDSD's overall data strategy.

8.9. Data Creators.

- a) Shall be responsibility for identifying new, freshly created pieces of data.
- b) Shall be responsible to gather, organise and share their explicit and tacit knowledge.

- c) Shall define their key knowledge goals that are aligned to ECDSD objectives and goals.
- d) Shall continuously update their own profile in the staff directory.
- e) Shall attend knowledge sharing session organised by Knowledge Management Champions

8.10. Security Manager

- a) Shall ensure that a comprehensive information classification system is developed and implemented by ECDSD.
- b) Shall ensure that all sensitive information produced or processed by ECDSD is identified, categorised and classified according to source origin, contents, and sensitivity.
- c) Shall ensure that electronic data are classified and only accessible to authorised users.

8.11. Deputy Director: Knowledge Management shall:

- a) Implement ECDSD's knowledge management strategy.
- b) Facilitate the translation of individual knowledge to corporate intellectual capital.
- c) Develop and implement effective Knowledge Management processes and systems.
- d) Create information sharing platforms.
- e) Promote Knowledge Management in and create a learning environment for ECDSD.
- f) Translate user needs into knowledge management requirements.
- g) Conduct case studies and produce meaningful reports.
- h) Analyse the data to discover its real meaning and use.
- i) Capture and codify knowledge to facilitate its reuse.
- j) Involve the knowledge workers and data producers and clean data at its source database.
- k) Publish reports on the Intranet through BI Dashboard and other reporting tools.
- l) Serve as a resource for organisational change management.
- m) Coordinate Departmental Knowledge Management Forum and participate in the Records Management Forum.
- n) Manage knowledge management projects.

8.12. Knowledge Management Champions shall:

- a) Act as information point of contacts within strategic Business units.
- b) Identify success stories for knowledge sharing.
- c) Provide requested information for the forum.
- d) Provide best practice in the forum secretariat.
- e) Connect colleagues who need information with sources of appropriate information and knowledge.
- f) Maintain information and knowledge connections with a variety of interest groups.

- g) Act as conduits of information and knowledge dissemination for their colleagues.
- h) Liaise closely with ECDSD.
- i) Participate in various communities of practice and fulfil knowledge brokering roles for colleagues in their divisions.

8.13. Director: Information Management Service

- a) Shall facilitate the development and review of the Information Management and Data Governance Policy.
- b) Shall develop and implement this policy and procedures on behalf of the Accounting Officer within the requirements of ECDSD Policy Development Framework.
- c) Shall undertake appropriate consultation before submitting the policy and procedures to the Accounting Officer for formal endorsement / approval.
- d) Shall ensure that Information Management and Data Governance Policy is operationalised.
- e) Shall conduct reviews of policy and procedures in their designated areas, as required by ECDSD Policy Development Framework.
- f) Shall be responsible for the proper management and protection of knowledge generated and stored within the Electronic Knowledge Management systems.
- g) Shall work in conjunction with the Knowledge Management Unit to ensure that all knowledge management resources are kept up to date.

8.14. Director: Systems Development and Maintenance

- a) Shall be responsible for the day-to-day maintenance of the electronic data classification systems.
- b) Shall ensure that appropriate classification systems, technical manuals and systems procedures manuals are designed for each electronic system.
- c) Shall ensure that Departmental systems are designed with functionality that improves the quality of data captured.

8.15. Director: ICT Engineering and Infrastructure

- a) Shall be responsible for maintaining and backing up the systems, databases, and servers that store the ECDSD's data.
- b) They shall be responsible for the technical deployment of all the rules established by data owners to ensure rules applied within systems are working.

8.16. Chief Information Officer

- a) Shall play a crucial role in a data classification process by overseeing the development, implementation, and ongoing management of the policy.

- b) Shall ensure that data classification process within ECDSD is properly done and protected according to its sensitivity level.
- c) Shall coordinate development of data definitions and standards for data classification elements.
- d) Shall safeguard data by ensuring appropriate access.
- e) Shall ensure the ICT infrastructure enables knowledge creation, capturing and dissemination.
- f) Shall organise, integrate and coordinate technical, departmental and human resources for effective implementation of the policy.

8.17. ICT Governance Management

- a) Shall be responsible for assessment of the policy implementation and advising generally on information security controls.
- b) Working in conjunction with other corporate functions, it shall be responsible for running educational activities on ICT policies and cyber security to raise awareness of the responsibilities identified in the Information Management and Data Governance Policy.

8.20. THE HEAD OF DEPARTMENT

- a) The Head of Department of the ECDSD in conjunction with the Chief Information Officer shall implement, enforce and monitor the controls in accordance with the requirements outlined by Information Management and Data Governance policy.

THE MEMBER OF THE EXECUTIVE COUNCIL

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

9. EFFECTIVE DATE OF THE POLICY

This policy shall be implemented from its effective date approval.

10. 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.

11. ENFORCEMENT

- a) Failure to comply with this policy shall result in disciplinary action, which shall include termination of employment.
- b) Any conduct that interferes with the normal and proper operation of ECDSD's ICT systems, shall constitute violation of approved Information Management and Data Governance Policy
- c) ECDSD executive management reserves the right to revoke the privileges of users.

12. POLICY REVIEW

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

13. POLICY RECOMMENDATIONS AND APPROVAL

RECOMMENDED/NOT RECOMMENDED



MR. M. MACHEMBA

HEAD OF DEPARTMENT

DEPARTMENT OF SOCIAL DEVELOPMENT

DATE: 08/08/2026

APPROVED/NOT APPROVED



MS. B. FANTA

MEMBER OF THE EXECUTIVE COUNCIL

DEPARTMENT OF SOCIAL DEVELOPMENT

DATE: 17/08/2026