Province of the
EASTERN CAPE
SOCIAL DEVELOPMENT

ICT Service Management Policy

Department of Social Development

Policy Registration 2026-07

TABLE OF CONTENTS

1. TERMS AND DEFINITIONS

Term	Definition
Access	A mechanism or method enabling an authorised user to gain entry to, or utilise, a system or corporate resource.
Accountability	The obligation of an individual or entity to accept responsibility for their actions, decisions, and behaviour.
Administrator	An individual designated to manage user identities, roles, credentials, and the allocation of organisational resources and services.
Basic	A baseline configuration that meets the minimum established technical standards required by the Department.
Cloud	A network of remote servers hosted on the internet used to store, manage, and process data, as opposed to utilising a local server or a personal computer.
Electronic Communication	Any communication transmitted via email, fax, telephone, or the internet.
End User	The individual who ultimately utilises the information, devices, systems, or software provided by the Department.
Executive Management	The strategic decision-making body of the Department, consisting of the Accounting Officer, Deputy Director-General, Chief Directors, and members of the Senior Management Service (SMS) level.
Gigabyte	A standard unit of digital data storage capacity equal to 1,024 megabytes.
Government Information Technology Officer (GITO)	The official responsible for aligning the Eastern Cape Department of Social Development's (ECDSD) ICT strategic plan, its strategic direction, and its operational management plans with provincial and national mandates.
Head of Department	The appointed Head of Department and Accounting Officer for the Eastern Cape Department of Social Development.
Internal Server	A server hosted physically within the primary premises of the ECDSD, rather than being hosted by an external agency such as the State Information Technology Agency (SITA).
Internet Protocol Security (IPsec)	A secure framework of protocols used to protect network traffic over an Internet Protocol network by authenticating and encrypting data packets.
Member of the Executive Council	The executing authority appointed by the Premier to provide political leadership and oversight to the Provincial Department.
Personal Computer (PC)	A general-purpose computer designed for independent use by a single end user within an office environment.
Personal Digital Assistant (PDA)	A legacy term for a portable, handheld device that functions as a mobile personal information manager.

Secure Shell (SSH)	A cryptographic network protocol used for operating network services securely over an unsecured network, typically establishing an encrypted link between a server and a client.
Server	A computing device on a network that dedicatedly manages network resources, hosts applications, or provides data and services to clients and end users.
Server Hosting	The physical or virtual placement, environment, and infrastructure where a server is located and maintained.
Service Catalogue	A structured, authorised, and comprehensive list of all IT services available to internal or external customers, providing clear details regarding service descriptions, service levels, eligibility, and the request process.
Acronyms	
GB	Gigabyte
CIO	Chief Information Officer
ECDSD	Eastern Cape Department of Social Development
GITO	Government Information Technology Officer
ICT	Information and Communication Technology
SSH	Secure Socket Shell
IPSec	Internet Protocol Security
PC	Personal Computer
PDA	Personal Digital Assistant
OH&S	Occupational Health and Safety

2. LEGISLATIVE FRAMEWORKS

a) Constitution of the Republic of South Africa (Act 108 of 1996)
b) Public Finance Management Act (Act No. 1 of 1999)
c) The Promotion of Access to Information (Act No. 2 of 2000)
d) The Promotion of Administrative Justice (Act No. 3 of 2000)
e) Promulgated Regulations in terms of the Protection of Personal Information (Act No.4 of 2013)
f) The State Information Technology (Act No. 88 of 1998)
g) South African Bureau of Standards/International Standardisation Organisation (SABS/ISO 17799 (2005)
h) Minimum Information Security Standards (MISS 1996)
i) Guidelines for the Handling of Classified Information (SP/2/8/1)
j) Electronic Communications and Transaction (Act No. 25 of 2002)
k) State Information Technology Agency (Act No. 88 of 1998)
l) The Regulation of Interception of Communications and Provision of Communication-Related Information (Act 70 of 2002)
m) National Cloud Computing Legislation Principles: Guidance for Public Sector Authorities Moving to the Cloud, 2015
n) Private Security Industry Regulation (Act 56 of 2001)

3. PREAMBLE

The Department of Public Service and Administration (DPSA) has issued Circular No.12 of 2026, introducing the IT Service Management Policy Guidelines for the Public Service along with an Implementation Framework. This circular sets out standards for managing IT services across government departments to improve efficiency, accountability, and service delivery.

This ICT Service Management (ICTSM) Policy establishes the framework for the effective planning, delivery, support, and continual improvement of ICT services in alignment with organisational objectives and business needs. This policy adopts recognised good practice principles, including ITIL and COBIT, to ensure that ICT services are reliable, secure, customer-focused, and delivered in a consistent and controlled manner. It defines governance requirements, roles, and processes necessary to manage ICT services throughout their lifecycle while promoting accountability, service quality, risk management, and value optimisation for the organisation and its stakeholders.

4. PURPOSE

The purpose of the policy is to provide a guiding framework on processes and procedures of basic ICT Service Management.

5. OBJECTIVES

a) To implement a structured process for improving service delivery to ICT clients.
b) To ensure service requests are recorded and evaluated in a controlled manner.
c) To create and maintain an effective relationship between ICT and clients.

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 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:** Department shall ensure employees take responsibility for actions and outcomes.

8. POLICY PROVISIONS

8.1. Conformity and Reporting

a) The ICT Service Management shall ensure changes to the departmental systems are planned and managed, consequences of unintended changes are reviewed, and action taken to mitigate adverse effects.

8.2. Service Requirements

a) A clear definition of service requirements shall be agreed and maintained with the clients of the ICT services.
b) Statutory, regulatory and contractual requirements for service management shall be documented and populated to the planning process.
c) Service requirements shall be regularly communicated to relevant stakeholders.
d) Authorised departmental mobile devices shall have ICT Service Management approved departmental systems installed.

8.3. Alignment with Business and Planning Cycle

(a) Shall ensure that IT Service Management objectives are defined during the annual budget planning cycle and are aligned with clearly understood business requirements and strategic priorities.

8.4. Funding and Continuous Improvement

(b) Shall ensure that IT Service Management objectives are supported by adequate funding to enable the implementation of continual service improvement initiatives identified through service performance assessments and customer reviews.

8.5. Governance and Documentation

(a) Shall ensure that all IT Service Management objectives are formally documented in the approved Service Management Plan for the relevant financial year, together with clear actions, responsibilities, and performance measures for successful achievement.

8.6. Service Reporting

a) The service reporting shall be produced by ICT Service Management to inform business service levels.

8.7. Service Level Management

(a) Shall ensures that ICT services are delivered and continuously improved through formally agreed Service Level Agreements (SLAs) aligned to business requirements.

(b) All IT services shall be governed by an approved SLA defining measurable service targets, performance metrics, workload limits, reporting frequencies, and exceptions.
(c) SLAs shall be developed collaboratively between the Head of IT and business owners, formally approved and signed by all parties, reviewed at least annually or upon significant service or workload changes, and amended only through written agreement.
(d) Service performance against SLA targets shall be monitored and reported as specified, with failures investigated and addressed through corrective actions or service improvement plans.
(e) All underpinning contracts, Operational Level Agreements (OLAs), and the service catalogue shall be aligned with SLAs to ensure service targets are achievable and business needs are met.

8.8. Supplier Management

(a) All supplier services shall be covered by formal contracts that define service scope, responsibilities, service levels, and supplier relationships.
(b) Contracts shall be securely stored, reviewed periodically, and amended through formal management processes.
(c) Supplier interactions and performance shall be managed through defined interfaces, regular communication, and ongoing monitoring, with contract disputes recorded and resolved by the service management function.

8.9. Incident Management

(a) All incidents shall be identified, logged, categorised, prioritised, diagnosed, resolved, and formally closed to minimise business impact, ensure user satisfaction, and support continual service improvement.

8.10. Service Catalogue

(a) The Department shall maintain a service catalogue that provides an approved and accurate description of all ICT services offered to internal and external customers.
(b) The service catalogue shall define each service's scope, value, availability, and associated roles and responsibilities, and shall be used to support effective communication, service transparency, and alignment between ICT and business requirements.

8.11. Problem Management

The ICT Department shall manage problems throughout their lifecycle by investigating underlying causes, implementing permanent or temporary solutions, and maintaining known error records to improve service stability and support continual service improvement.

8.12. Change Management

(a) Shall ensure that all changes to ICT systems, applications, and infrastructure are recorded, assessed, authorised, and implemented in a controlled manner to minimise risk and maintain service stability.
(b) All changes, including emergency changes, shall require formal approval prior to implementation, with emergency changes permitted only for critical business disruptions and authorised by the Head of IT.

8.13. Project Management

(a) Shall ensure that ICT service–related projects are planned and delivered in a controlled manner within approved cost, time, and quality parameters, using the department's approved project management methodology.

8.14 Asset Management

(a) ICT Asset Management (ITAM) shall ensure that all ICT assets are identified, recorded, deployed, maintained, upgraded, and retired in a controlled manner throughout their lifecycle, in accordance with the department's approved asset management policy, to support effective service delivery, compliance, and value optimisation.

8.15. Client / Customer Management

b) Shall ensure that the ICT branch establishes and maintains effective relationships with customers to understand their needs and ensure ICT services deliver value. This shall be achieved through structured communication, service reviews, complaint handling, customer satisfaction measurement, and regular feedback to support continual service improvement and alignment with business objectives.

9. APPROVING AUTHORITY

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

10. ACCOUNTABILITIES AND RESPONSIBILITIES

10.1. Director: ICT engineering and Infrastructure

Shall implement, enforce and monitor the controls in accordance with the requirements outlined by management, and shall advise users on the correct ways to access information and systems.

10.2. ICT Engineering and Operations

The ICT Engineering and Operations shall be responsible for maintenance and advising on information security controls, reviewing the configuration and approving configuration requirements and changes, working in conjunction with other ICT business units.

10.3. The Head of Department

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 management.

10.4. The Member of the 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

CIO 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.

13. 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 departments ICT systems, shall constitute violation of the approved ICT Service Management Policy.
c) The Department executive management reserves the right to revoke the privileges of users.

14. POLICY REVIEW

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

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

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