Province of the
EASTERN CAPE
SOCIAL DEVELOPMENT

ICT INFRASTRUCTURE POLICY

Department of Social Development

Policy Registration 2026-06

TABLE OF CONTENTS

TERMS AND DEFINITIONS

Terms	Definitions
Access	The granting of permission to use, view, or enter a specific ICT system, network, or physical facility.
Accountability	The requirement for actions and decisions to be traceable to a specific individual, ensuring that responsibilities are met and consequences can be applied.
Control	A measure used to modify or manage risk, encompassing policies, procedures, technical configurations, and physical safeguards.
Datacentre	A highly secure physical facility equipped with redundant power, cooling, and fire suppression to house critical servers and networking equipment.
Demilitarised Zone	A logical sub-network that separates an internal private network from untrusted external networks (the Internet) to protect public-facing services.
Electronic Data Interchange (EDI)	The automated, computer-to-computer exchange of business documents in a standardised electronic format.
Encryption	The cryptographic process of converting data into an unreadable format (ciphertext) to ensure confidentiality and integrity.
End User	Any authorised official, contractor, or third party utilising Departmental ICT resources to perform official duties.
Environment Hazard	A physical state or event (e.g., flooding, overheating, or chemical leaks) with the potential to damage ICT infrastructure or disrupt service availability.
Firewall	A security system (hardware or software) that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
Information Assets	Any identifiable data, knowledge, or intellectual property (e.g., databases, records) that holds value for Departmental operations.
Information Security	The preservation of the Confidentiality, Integrity, and Availability (CIA) of information through administrative, technical, and physical safeguards.
Legacy Systems	An ageing ICT system or application that remains in use because it performs a critical function, despite lacking modern security features or support.
Logical Access Control	Technical mechanisms, such as passwords or biometrics, used to authenticate and authorise users within digital environments.
Malicious Software	Also known as 'Malware' (including viruses, ransomware, and worms), designed to infiltrate or damage a computer system without informed consent.
Physical Access Control	The use of tangible barriers (locks, biometric scanners, security guards) to prevent unauthorised entry into restricted ICT areas.
Service Level Agreement (SLA)	A formal contract between a service provider and the Department defining expected performance levels, uptime, and recovery timeframes.

Threat	A potential cause of an unwanted incident which may result in harm to a system or the organisation.
Virtual Private Network (VPN)	A secure, encrypted 'tunnel' that extends a private network across a public network, allowing remote users to access internal resources safely.
Vulnerability	A weakness in an asset or security control that can be exploited by one or more threats to cause a breach.
ACRONYMS	
CIO	Chief Information Officer
DMZ	Demilitarised Zone
HOD	Head of Department
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information and Communication Technology
IDS	Intrusion Detection System
IMST Board	Information Management, Systems and Technology Board
IPSec	Internet Protocol Security
ISS	Information System Security
MEC	Member of the Executive Council
MIOS	Minimum Interoperability Standards
RM	Risk Management
SITA	State Information Technology Agency
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Socket Layer
UPS	Uninterrupted Power Supply
VPN	Virtual Private Network
WAN	Wide Area Network
WPA3 / WPA2	Wi-Fi Protected Access (Standard 3 or 2)

LEGISLATIVE FRAMEWORK

1. Constitution of the Republic of South Africa, 1996, as amended.
2. Disaster Management Act, 2002 (Act No. 57 of 2002), as amended.
3. Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002), as amended.
4. Guidelines for the Handling of Classified Information (SP/2/8/1), 1988
5. International Organisation for Standardisation (ISO/IEC 27001:2022 & 27002:2022)
6. Labour Relations Act, 1995 (Act No. 66 of 1995), as amended.
7. Minimum Information Security Standards (MISS), 1996
8. National Cloud Computing Policy, 2015 (and subsequent 2024 National Data and Cloud Policy updates).
9. Private Security Industry Regulation Act, 2001 (Act No. 56 of 2001), as amended.
10. Promotion of Access to Information Act, 2000 (Act No. 2 of 2000), as amended.
11. Promotion of Administrative Justice Act, 2000 (Act No. 3 of 2000), as amended.
12. Protection of Personal Information Act, 2013 (Act No. 4 of 2013), as amended.
13. Public Finance Management Act, 1999 (Act No. 1 of 1999), as amended.
14. Public Service Act, 1994 (Proclamation No. 103 of 1994), as amended.
15. Public Service Regulations, 2016, as amended.
16. Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act No. 70 of 2002), as amended.
17. SABS/ISO/IEC 27002:2022 (Information Security, Cybersecurity and Privacy Protection).
18. State Information Technology Agency Act, 1998 (Act No. 88 of 1998), as amended.

1. PREAMBLE

Following the review of the Infrastructure Security Policy, this document establishes mandatory standards for the secure configuration and use of all Departmental ICT systems, with a particular focus on the controls required for electronic communications. Recognising that e-mail is inherently insecure, and susceptible to interception, unauthorised modification, or legal misinterpretation, this policy secures the underlying network and server infrastructure to safeguard Departmental data. The Department is committed to providing robust ICT services to support its business functions; consequently, users must maintain professional behaviour that aligns with Departmental objectives. Adherence to these ICT policies and security requirements is a mandatory condition for the use of any Departmental facility or service.

2. PURPOSE

The primary purpose of this Policy is to establish mandatory standards for the secure configuration of ICT infrastructure and to define the acceptable use of these resources by all authorised users and administrators.

3. OBJECTIVES

The specific objectives of this Policy are:

a) **Wireless Security:** To implement robust security measures for both internal and external wireless network connections.
b) **Network Segmentation:** To ensure network devices are configured to effectively segment data and voice traffic for enhanced security and performance.
c) **Access Control:** To prevent unauthorised physical and logical access to the data centre, network infrastructure, and server rooms.
d) **Awareness and Compliance:** To ensure all employees are fully informed of the Department's standards regarding the acceptable and prohibited use of the e-mail system.

4. SCOPE OF APPLICABILITY

This Policy applies to all employees, contractors, third-party service providers, and any individuals granted access to Departmental ICT systems and infrastructure.

5. PRINCIPLES AND VALUES

The following core principles govern the implementation of this Policy and define the conduct expected of all users:

a) **Confidentiality**: Users shall uphold ethical and legal obligations to protect sensitive information from unauthorised disclosure, ensuring data is accessible only to those with a legitimate 'need-to-know'.
b) **Integrity:** Users shall maintain the accuracy and consistency of information and systems, ensuring that data is protected against unauthorised or accidental modification.

c) **Availability:** The Department shall implement resilient infrastructure to ensure that ICT systems and resources remain reliably accessible to authorised users in support of business functions.

d) **Accountability:** The Department shall maintain mechanisms to ensure that all users are held responsible for their actions and the resulting outcomes when using ICT facilities.

6. POLICY PROVISIONS

6.1. Interoperability and Governance

6.1.1. In accordance with the Public Service Regulations (2016), the Department shall adhere to the Minimum Interoperability Standards (MIOS). This includes compliance with technical specifications for interconnectivity, data integration, and information access across the public sector.

6.1.2. All information security measures shall follow the standards set by the Information Security Services (ISS) and Risk Management (RM) Committee, as endorsed by the Information Management Systems and Technology (IMST) Board.

6.2. Network Security and Connectivity

6.2.1. **Access Control**: Only authorised personnel shall have access to wiring closets and network rooms. All managed devices (routers, switches, print servers) must be protected by unique credentials and integrated into centralised system logging facilities.

6.2.2. **Untrusted Connections**: All connections to external or untrusted networks must be registered and authorised by ICT Management. Such connections must terminate on secure network nodes (e.g., VPN concentrators) using secure protocols (HTTPS/SSL).

6.2.3. **Perimeter Security**: Web, database, and payment servers accessible via the Internet must be protected by firewalls and placed within a Demilitarised Zone (DMZ), separate from internal subnets. Application-gateway (Layer 7) firewalls shall be utilised to protect traffic at the message level.

6.2.4. **SITA Integration**: Connectivity between internal networks and the Internet shall be managed by the State Information Technology Agency (SITA) as part of the WAN service, pursuant to the State Information Technology Act (1998).

6.2.5. **Prohibitions**: Users shall not establish unauthorised Intranets, bulletin boards, or modem connections. Computer systems containing 'Secret' classified information must never be connected to untrusted networks.

6.3. Wireless Security Standards

6.3.1. **Configuration**: Vendor default settings must be changed before deployment. Access points must use the highest available encryption (WPA3 or WPA2-AES) and complex shared secret keys.

6.3.2. **SSID and Segmentation**: Default SSIDs must be changed to approved naming conventions. Guest users must be restricted to a 'Guest' SSID with no access to internal resources.

6.3.3. **Monitoring**: Intrusion Detection Systems (IDS) must be enabled on all wireless access points to detect and mitigate threats.

6.4. Physical and Environmental Controls

6.4.1. **Physical Access**: Critical information processing facilities must be housed in secure areas protected by defined perimeters and entry controls. Access registers must be maintained for all data centres.

6.4.2. **Environmental Protection**: Data centres must be equipped with:

a) Raised flooring for flood protection.

b) Air conditioning for temperature and humidity control.

c) Fire detection and suppression systems (regularly maintained).

d) Uninterrupted Power Supplies (UPS) with lithium-based batteries.

6.4.3. **Prohibitions**: Flammable materials and hazardous chemicals are strictly prohibited within data centres and network rooms.

6.5. Infrastructure Maintenance and Changes

6.5.1. **Cabling and Installations**: Network cabling requests require a minimum of three years remaining on a building lease. All work must comply with Departmental cabling standards.

6.5.2. **Assessments**: The Department shall conduct comprehensive infrastructure assessments across all Local Service Offices and districts at least once per financial year.

6.5.3. **Authorisation**: Only the IT Department is authorised to modify network access points. No equipment may be moved or removed from premises without explicit, documented permission from ICT Management.

6.6. E-mail Usage and Security

6.6.1. **Professional Conduct**: E-mail is for business purposes. Users must not send offensive, defamatory, racist, or illegal content. Limited personal use is at the discretion of management, provided it is incidental and does not interfere with operations.

6.6.2. **Security Controls**: Sensitive information must be encrypted before transmission. Users are prohibited from using personal 'Webmail' (Gmail, Yahoo, etc.) for official business or auto-forwarding corporate e-mail to external accounts.

6.6.3. **Data Ownership**: All e-mails processed by Departmental systems are the property of the organisation. The Department reserves the right to scan, archive, and audit e-mails for security purposes.

6.6.4. **Account Lifecycle**: E-mail accounts shall be terminated within 24 hours of notice from HR, or following 30 days of inactivity for new accounts, or six months of general inactivity.

6.7. Server Security Policy

6.7.1. **Classification**: Servers are categorised as Critical (hosting sensitive/financial data), User Account Services, or Non-Core (testing/research).

6.7.2. **Management**: All internal servers must be owned by the ICT Directorate. Critical servers must be centrally hosted in a secured SITA Data Centre or ICT Computer Room.

6.7.3. **Hardening**: Servers must be 'hardened' by disabling unnecessary services. Security patches must be applied as soon as practically possible.

6.7.4. **Access**: Privileged access (administrator rights) must be kept to a minimum and performed over secure, encrypted channels (SSH/IPSec). The use of 'Guest' accounts is prohibited.

6.7.5. **Content**: The storage of pirated music, video, or software on any Departmental server is strictly prohibited.

7. APPROVING AUTHORITY

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

8. ACCOUNTABILITIES AND RESPONSIBILITIES

8.1. The Member of the Executive Council (MEC)

The MEC is responsible for the formal approval of this Policy and providing the necessary political oversight to ensure alignment with provincial and national mandates.

8.2. The Head of Department (HOD)

The HOD, supported by the ICT Head/CIO, is accountable for the overall implementation of this Policy and for ensuring that the Department maintains effective compliance with all associated internal standards and procedures.

8.3. The Information Management Systems and Technology (IMST) Board

The IMST Board is responsible for the strategic oversight of ICT security. This includes endorsing security standards, approving high-risk network connections, and ensuring that ICT initiatives align with the Department's broader business objectives.

8.4. The Chief Information Officer (CIO)

The CIO shall implement, enforce, and monitor technical controls in accordance with management requirements. The CIO is further responsible for advising users on the secure access of information and systems.

8.5. ICT Governance

ICT Governance is responsible for assessing policy implementation and providing specialist advice on information security controls. In collaboration with other corporate functions, this unit shall conduct educational and awareness programmes regarding cyber security, phishing, and the acceptable use of e-mail and social media.

8.6. ICT Infrastructure and Operations

ICT Infrastructure and Operations is responsible for the technical deployment, maintenance, and management of the security controls governing the Department's networks, servers, and hardware.

8.7. Employees and Authorised Individuals

All Departmental employees, contractors, and individuals granted access to systems are responsible for adhering to the provisions of this Policy. Non-compliance may result in the revocation of access and disciplinary action.

9. EFFECTIVE DATE OF THE POLICY

This policy shall be implemented from its effective date of approval.

10. MONITORING MECHANISMS

The ICT Head and Senior Management shall be required to ensure the ICT Operational Committee, the ICT Steering Committee and the 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 the Department's ICT systems, shall constitute a violation of the approved Infrastructure Security Policy.

c) The Department's executive management reserves the right to revoke the privileges of users.

12. POLICY REVIEW

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

13. POLICY RECOMMENDATION AND APPROVAL

RECOMMENDED/NOT RECOMMENDED

MR M. MACHEMBA

HEAD OF DEPARTMENT

EASTERN CAPE DEPARTMENT OF SOCIAL DEVELOPMENT

DATE: 28/06/2020

APPROVED/NOT APPROVED

MS B. FANTA

MEMBER OF THE EXECUTIVE COUNCIL

EASTERN CAPE DEPARTMENT OF SOCIAL DEVELOPMENT

DATE: 11/08/2020