Province of the
EASTERN CAPE
SOCIAL DEVELOPMENT

Access Management Policy

Department of Social Development

Policy Registration 2026-01

TABLE OF CONTENTS

1. TERMS AND DEFINITIONS 2

2. LEGISLATIVE FRAMEWORKS 5

3. PREAMBLE 6

4. PURPOSE 6

5. OBJECTIVES 6

6. SCOPE OF APPLICABILITY 6

7. PRINCIPLES AND VALUES 7

8. POLICY PROVISIONS 7

9. APPROVING AUTHORITY 14

10. ACCOUNTABILITIES AND RESPONSIBILITIES 14

11. EFFECTIVE DATE OF THE POLICY 15

12. MONITORING MECHANISMS: 15

13. POLICY REVIEW 16

14. ENFORCEMENT 16

15. POLICY APPROVAL 17

TERMS AND DEFINITIONS

Terms	Definitions
Access	The ability or permission to use, enter, or communicate with a system or physical environment.
Accountability	The obligation of an individual or entity to account for its activities, accept responsibility for them, and disclose the results in a transparent manner.
Asset	A resource, physical or intangible, controlled by the Department from which future economic or service benefits are expected to flow.
Control	Any action, policy, procedure, or professional structure used by management to manage risks and increase the likelihood that established objectives and goals will be achieved.
Database	A structured set of data held in a computer, especially one that is accessible in various ways, ranging from simple desktop systems to complex, multi-machine implementations.
Datacentre	A centralised physical facility that houses critical computing resources, including servers, routers, switches, firewalls, and supporting infrastructure such as power backups and environmental controls.
Electronic Communications	Any transfer of signs, signals, writing, images, sounds, or data transmitted via systems such as email, intranet, internet, and telephony.
Encryption	The process of converting information or data into a code, especially to prevent unauthorised access, ensuring confidentiality and integrity.
End-User	An official or authorised individual who utilises the information, computer equipment, and systems of the Department to perform their duties.
Environment Hazard	A substance, state, or event (such as fire, flood, or chemical leak) with the potential to threaten the surrounding environment or adversely affect human health and ICT infrastructure.
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.
Firewall	A network security device that monitors and filters incoming and outgoing network traffic based on an organisation's previously established security rules.
Generic Accounts	Shared computing accounts created for specific functional purposes rather than assigned to a unique individual, often used by multiple administrators or guests.
Gigabyte	A standard unit of measurement for data storage capacity, equal to 1,024 Megabytes.
Government Information Technology Officer	The executive official responsible for the Information Technology strategy and the systems required to support the Department's strategic objectives.
Head of Department	The Accounting Officer of the Eastern Cape Department of Social Development, as defined by the Public Finance Management Act.
ICT Steering Committee	A high-level governance body responsible for overseeing ICT processes, ensuring alignment between IT strategy and business goals, and monitoring resource investment.
Information Assets	Knowledge or data that has value to the Department, including the physical hardware, software, and communication devices used to store or transmit it.
Information Communication and Technology	An umbrella term that includes all technologies for the communication of information, encompassing the integration of telecommunications, computers, and enterprise software.
Information Security	The practice of protecting information by mitigating information risks, including organisational, technical, and social measures to prevent unauthorised access or damage.

Terms	Definitions
Internal Audit	An independent, objective assurance and consulting activity designed to add value and improve the Department's operations by evaluating the effectiveness of risk management and controls.
LAN (Local Area Network)	A computer network that interconnects computers within a limited area such as a single building or office suite.
Member of the Executive Councillor	The Executive Authority appointed by the Premier to provide political leadership and oversight to the Provincial Department.
Password	A confidential string of characters used for user authentication to prove identity or approve access to a resource.
Personal Computer	A multi-purpose computer whose size, capabilities, and price make it feasible for individual use by an end-user.
Personal Digital Assistant	A legacy term for a mobile device that functions as a personal information manager; in modern contexts, this typically refers to smartphones or tablets.
Physical Access	The ability of personnel to physically reach and interact with ICT equipment, server rooms, or secure facilities.
Relationship	The defined associations or permissions that exist between specific users and departmental resources.
Remote Sources	External entities, networks, or locations outside the Department's primary network that may pose security threats.
Resources	Specific components within a system (data, hardware, or software) that require protection and controlled access.
Router	A networking device that forwards data packets between computer networks, typically connecting a LAN to a Wide Area Network (WAN).
Server Room	A controlled, secure environment dedicated to housing servers and data storage devices.
Service Level Agreement	A formal contract between a service provider and the Department that specifies the standards of service, responsibilities, and penalties for non-compliance.
Third-Party Employees	Personnel employed by an external service provider or contractor who are engaged to perform specific services for the Department.
WAN (Wide Area Network)	A telecommunications network that extends over a large geographical area, often used to interconnect various LANs across different districts or cities.
ACRONYMS	
AG	Auditor General
BAS	Basic Accounting System (BAS)
CCTV	Closed-Circuit Television
CD	Compact Disc
CIO	Chief Information Officer
COBIT	Control Objectives for Information and Related Technology
DRP	Disaster Recovery Plan
DVD	Digital Video Disc
ECDSD	Eastern Department of Social Development
E-mail	Electronic Mail
ERM	Enterprise Risk Management
GB	Gigabyte
GITO	Government Information Technology Officer
HOD	Head of Department
HRA	Human Resource Administration

Terms	Definitions
ICT	Information and Communication Technology
ID	Identification
IOS	Internet Operating System
ISF	Information Security Forum
ISM	Information Security Manager
ISP	Internet Service Provider
IT	Information Technology
ITIL	Information Technology Information Library
MFA	Multifactor Authentication
MISS	Minimum Information Security Standard
OTP	Office of the Premier
PC	Personal Computer
PDA	Personal Digital Assistant
PERSAL	Personnel and Salary System (PERSAL)
SDIMS	Social Development Information Management System
SITA	State Information Technology Agency
SLA	Service Level Agreement
SMS	Senior Management Service
USB	Universal Serial Bus

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 Administrative Justice Act, 2000 (Act No. 3 of 2000)
4. Promotion of Access to Information Act, 2000 (Act No. 2 of 2000)
5. Protection of Information Act, 1982 (Act No. 84 of 1982)
6. Protection of Personal Information Act, 2013 (Act No. 4 of 2013)
7. State Information Technology Agency Act, 1998 (Act No. 88 of 1998)
8. SABS/ISO 17799 (2005): South African Bureau of Standards / International Organisation for Standardisation
9. Minimum Information Security Standards (MISS), 1996
10. Guidelines for the Handling of Classified Information (SP/2/8/1)
11. Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002)
12. Public Service Act, 1994 (Proclamation No. 103 of 1994)
13. Public Service Regulations, 2016
14. ISO/IEC 27001:2005: International Organisation for Standardisation
15. Regulation of Interception of Communications and Provision of Communication-related Information Act, 2002 (Act No. 70 of 2002)
16. Disaster Management Act, 2002 (Act No. 57 of 2002)

1. PREAMBLE

The protection of the Department's information assets is fundamental to ensuring operational integrity, consistent service delivery, and full compliance with applicable legislative and regulatory frameworks. The proliferation of Information and Communication Technologies (ICT) necessitates the implementation of robust controls to govern how users access systems, applications, and data, particularly within environments containing sensitive information or critical ICT assets.

The Access Management Policy establishes a secure and standardised approach to the authorisation, modification, review, and revocation of access rights. This framework ensures that individuals are granted only the permissions necessary to perform their assigned duties, adhering to the principle of least privilege to prevent unauthorised system use, mitigate cybersecurity threats, safeguard sensitive personal information, and maintain the confidentiality, integrity, and availability of departmental resources.

This policy is aligned with recognised ICT governance and security frameworks. It supports departmental compliance with key legislation, notably the **Protection of Personal Information Act (Act No. 4 of 2013) (POPIA)**. Through this policy, the organisation affirms its commitment to the responsible, accountable, and secure management of user access to information and technology resources.

Following a comprehensive review process, the scope of this policy has been extended to encompass a full range of access management controls. These include both logical and physical access controls pertaining to departmental data, information systems, networks, business applications, and physical facilities.

2. PURPOSE

The purpose of this Policy is to ensure that all users are granted access rights appropriate to their roles, responsibilities, and business needs, while protecting organisational information systems from unauthorised use, data breaches, and security risks by conforming to user access management best practice standard controls.

3. OBJECTIVES

a) To define the user access management control measures for departmental ICT systems.
b) To protect privacy and security information.
c) To ensure confidentiality, integrity, and availability of departmental information assets.
d) To authorise users to perform their duties effectively.

4. SCOPE OF APPLICABILITY

This Policy applies to all employees, contractors, auditors, investigators, vendors, and third-party entities granted access to ECDSD's information systems, networks, applications, and physical facilities. It encompasses both electronic and physical access controls.

5. PRINCIPLES AND VALUES

a) **Confidentiality:** The Department's 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.

6. POLICY PROVISIONS

6.1. User Account Management

6.1.1. Privileged Access Right

a) The number of employees having elevated rights shall be kept to a minimum as per Access Management Policy and a record of such employees shall be kept.

b) Access to operating system commands shall be restricted to ICT Officials, who are authorised to perform systems administration functions.

6.1.2. Review and Monitoring of Access

a) Access to the Department's information assets shall be logged and monitored on a continuous basis.

b) Logs of access to critical departmental systems, network and applications shall be kept for a period of twelve months.

c) Logs to departmental systems shall be:

   i. Reviewed regularly to help identify suspicious or unauthorised activity by the password administrator.

   ii. Retained for at least a three-month period to investigate past activities.

   iii. Protected against unauthorised changes.

d) A formal record of all registered users in the department shall be maintained and monitored.

6.1.3. User Registration

a) Granting of access to generic accounts (service accounts) shall be strictly controlled.

b) A formal document (e.g., a User Registration Form) shall be completed by each user.

c) The form shall be legally approved with all requirements stated on the form.

d) Each user shall be assigned a unique user ID. This shall be:

   i. A Persal Number.

ii. The First 8 or last 8 digits of the user's ID if there is no Persal number assigned.

iii. An Employment number in case of external service providers or First 8 or last 8 digits of user's ID if there is no Persal number provided.

e) For contract-worker users and individual users granted access, the end date shall be included on creation.

6.1.4. User Modifications

a) Each user shall complete a User Modification Form.

b) The change needed shall be specified by the owner.

c) Where there is a change of personal information (e.g., ID number, Surname and Persal Number), Human Resource Administration shall first approve.

d) Where the user needs to be activated after deactivation due to suspension or contract expiry and renewal, HRA shall first approve.

e) If a category of users has been deleted, a new User Creation Form shall be submitted.

f) Additional access rights shall be approved by a supervisor.

6.1.5. User Termination

The ICT Unit, upon receiving an authorised retirement notification from HRA, shall immediately initiate the deactivation of all user accounts, revoke system privileges and disable login credentials:

a) Users shall be terminated within one day after receiving information from HRA to terminate the user.

b) Users shall be terminated when they have not logged in for thirty days after they have been created.

c) Users shall be terminated when they have not logged in for a period of ninety days.

d) User shall be deactivated in the event of an extended leave.

e) Users shall no longer have access once terminated.

f) Users requesting access to a previous mailbox and or documents shall be granted through a memo approved by the Accounting Officer or delegated official with the timeframe for the account activation clearly specified.

6.2. Password Management

6.2.1. Issuing a New or Changing a Password

When issuing a new password or when changing passwords, it shall be ensured that:

a) The initial password is transferred to the individual telephonically or by email, which shall be changed upon first use.

b) The disclosure of passwords is minimised when they are communicated to the user.

c) The display and printing of passwords is masked, suppressed, or otherwise obscured so that unauthorised parties are unable to observe or subsequently recover the passwords.

d) It involves the target user directly (i.e., The person to whom the password uniquely applies).

e) The identity of the target user is verified (e.g., Via a special code or through independent confirmation).

6.2.2. Authorised Third Parties

Where passwords are displayed to authorised third parties, for example to a security administrator, the following conditions shall be met:

a) Users shall be required to change the password at first login.

b) Functions and information accessed through using the password shall have been classified as low sensitivity by the Department.

6.2.3. Password Recovery, Reissuing and Maintenance

A procedure for providing users who have forgotten their passwords with new passwords shall be in place. This procedure shall include the following elements:

a) The issuing of temporary passwords telephonically or through email to the user after a positive identification.

b) The requirement that the user changes the temporary password immediately.

c) The requirement that the user updates their password when they suspect or believe it has been compromised.

f) The requirement that passwords are changed at least every forty-two days.

g) The issuing of unique passwords held by the user of the account when users have system-level privileges granted through group membership.

h) The use of Self-Service Password Reset when implemented.

i) The use of a different email address or SMS receiving cell phone number for Multi-Factor Authentication.

6.2.4. Password Security

a) A password shall never be disclosed to any third party.

b) All passwords shall have at least 8 lower and uppercase symbols, mixed with alpha-numeric and special characters.

c) The last six passwords shall not be reusable.

d) A period of fifteen days between password changes shall be set to ensure users do not change passwords several times in a row to return to known old password.

e) In order to prevent unauthorised access to other user's computers, information or data, requests to reset passwords shall be strictly and constantly monitored.

f) System administrators shall not reset a password unless the user has logged the call with ICT Helpdesk and has duly completed the password reset form.

6.2.5. Password Storage

a) Passwords shall only be stored in encrypted form using a strong one-way encryption algorithm.

b) Passwords shall not be stored in readable form in batch files, automatic log-in scripts, software macros, terminal function keys, or in other locations where unauthorised users might discover or use them, except with the formal permission of the ISM.

6.2.6. Legacy Systems and Applications

Certain legacy systems constrain the length of passwords, or the characters that shall be used, to the extent that the passwords cannot conform to the contemporary definition of a secure password. These systems shall continue to operate with the less secure passwords through the approval of the Information Security Manager or the Risk Management Committee. This shall be so under the following conditions:

a) The system is in the process of being decommissioned, or steps are being taken to correct the situation.

b) The functions and information exposed to the users has been classified as low sensitivity by the ISM/RM Committee.

c) Steps have been taken to mitigate the risk, for example by isolating the system on the network and protecting access through an additional authentication layer.

d) The risk has been formally documented and accepted or transferred by the business/system/information user.

e) The systems support the authentication of individual users not groups.

f) The passwords are not transportable or communicable in clear text and in any easily reversible form.

6.2.7. Password Management System

a) Any systems that generate or store passwords shall do so securely. Where feasible, applications shall rely on operating system controls for authentication and authorisation.

b) Systems shall mask or obscure passwords while being entered.

c) ID numbers and passwords shall never be conveyed to users in the same communication.

d) Where enabled by operating systems and applications, the Department shall implement a password management system that has the following characteristics:

   i. The acceptance of individual user-ID's and passwords only, as opposed to shared accounts.

ii. The instruction to change passwords whenever there is any indication of possible system or password compromise.

iii. The enforcement of the selection of secure passwords only.

iv. Controls in place to prevent frequent password changes over a short period of time.

e) All sensitive information, including passwords, shall be encrypted with a departmental approved algorithm using at least 128-bit encryption prior to transmission over a network.

f) System-generated passwords shall be generated using a frequently changing unpredictable source and shall always be issued immediately after generation.

g) Unissued passwords and PINs shall never be stored, regardless of the form they take.

h) All computer storage media and computer memory areas used in the construction, assignment, distribution, or encryption of passwords or personal identification numbers, shall be erased using a departmental approved algorithm or equipment immediately after use.

6.2.8. Access Control

a) Application systems developers shall not develop authentication and access control systems where the controls provided by an operating system or an access control package that enhances the operating system shall be used. Designs featuring custom authentication and access control systems shall be authorised by ISM/RM Committee.

b) All workstations used for Department business activity, no matter where they are located, shall use an access control system approved by the ISM/RM Committee. This system shall lock access to the workstation after a period of inactivity.

c) Log-in process for multi-user computers shall include a special departmental Information Security notice.

d) Following installation of hardware or software, all default vendor passwords shall be altered.

e) If sent by regular mail or similar physical distribution systems, passwords shall be sent separately from user-ID. These mailings shall have no markings indicating the nature of the enclosure. Passwords shall also be concealed inside an opaque envelope that will readily reveal tampering.

6.2.9. Security Administrators

a) Security administrators shall only disclose passwords if a new user-ID is being assigned, if the involved user has forgotten or misplaced a password, or if the involved user is otherwise locked out of the user-ID.

b) Security administrators shall not reveal a password unless the involved user has first provided definitive evidence substantiating user identity.

6.2.10. User Conduct

a) All users shall keep their passwords confidential.

b) A user shall never keep a written copy of departmental passwords.

c) Users shall not share passwords.

d) A user will be held responsible for any actions secured with their user password.

e) Access control to files, databases, computers, and system resources via shared passwords is prohibited.

f) Procedures or security awareness training shall be in place for users of electronic equipment, including desktops, server consoles, mobile equipment.

6.2.11. Remote Access

a) Access to the departmental network via remote access shall be controlled using either one-time password authentication or public/private key system with strong pass phrase.

b) Pass phrase shall not be the same as user's passwords.

6.3. The Physical Environment

6.3.1. Identification and Authentication

All locations that house critical ICT facilities, sensitive material and other important assets shall be physically protected against accidents or attacks in order to restrict physical access to authorised individuals only, and to ensure that critical ICT facilities are available when required. These include computer rooms and data centres which the Department must protect to mitigate the possibility of the impact of damage from natural hazards, unauthorised access by employees, and unauthorised access by individuals granted access to departmental facilities. Consequently, buildings that house critical ICT facilities shall be protected against unauthorised access by:

a) Locks, bolts (or equivalent) on vulnerable doors and windows.

b) Employing security guards.

c) Installing Closed-Circuit Television (CCTV), or its equivalent.

d) Storing sensitive physical material (e.g., CDs, DVDs, External storage devices like hard-drives and USB memory sticks) in locked cabinets or drawers when not in use (e.g., by enforcing a 'clear desk' policy).

e) Restricting physical access to important post/facsimile points and locating equipment used for sensitive printed material in secure physical areas.

f) Requiring that all employees, contract workers and individuals granted access wear their name tags in the workplace to make their identities verifiable.

g) Requiring that ICT officials and employees report to security personnel when persons failing to display their name tags are found entering designated areas that store departmental Information and Technology Systems.

6.3.2. Authorisation and Access Control Management

Physical access to computer installations and server rooms shall be restricted from unauthorised individuals by the Chief Information Officer (CIO)/Head of ICT Infrastructure through:

a) Installing locks activated by keypads, swipe cards or an equivalent.
b) Locking doors and windows when the environment is vacated.
c) Fitting intruder alarms.
d) Ensuring all individuals wear name tags.
e) Requiring staff to report strangers and any unrecognised individual.
f) Employing security guards and using Access Control Registers during office hours.
g) Requiring the explicit permission of the CIO to access computer installations and the server rooms after official working hours.
h) Allowing only officially appointed contract workers and individuals granted access into server rooms as permitted by the CIO.
i) Ensuring that those granted permission are monitored by recording upon arrival and departure time and are supervised at all times.
j) Ensuring the issuing of instructions explaining the security requirements of the area, detailing emergency procedures and the prohibition of audio-visual recording.

6.3.3. Removal of Equipment and Physical Access Rights

a) Individuals shall be required to obtain written approval before leaving the workplace with non-mobile computer equipment (e.g., servers, desktops, network devices and printers).
b) A formal record of physical access rights shall be maintained by the Physical Security Manager.
c) Physical access rights to designated secure areas shall be reviewed and updated by the Information Owner on an annual basis (i.e., re-issue of keys, access codes or updating of access cards),
d) The Physical Security Manager shall promptly recover all name tags issued to users whose services are no longer required.
e) No departmental equipment or software shall be allowed to be taken off-site without prior written authorisation by the Information Owner.

6.3.4. Information Integrity and Recoverability

a) The ICT Steering Committee shall approve minimum specifications for secure areas (e.g., computer rooms, data centres, etc.), considering the impact and likelihood of damage to the Department's Information Technology Systems from natural hazards as well as unauthorised access by users.
b) All designated secure areas shall be suitably protected from damage through natural disasters. (e.g., by deploying suitable fire suppression systems and installing raised flooring and temperature control equipment).

6.3.5. Environmental Security

Rooms housing critical ICT facilities shall be:

a) Free from intrinsic fire hazards such as paper or chemicals.
b) Fitted with fire detection and suppression systems.
c) Protected against the spread of fire by using fire resistant doors and materials.

The impact of hazards shall be minimised by:

a) Locating hand-held fire extinguishers to minor incidents can be tackled without delay.
b) Training staff in the use of emergency-safety equipment, and emergency evacuation procedures.
c) Monitoring and controlling the temperature and humidity of computer rooms in accordance with equipment manufacturer recommendations.
d) Using uninterruptible power supplies.
e) Installing raised floor to protect against flooding.
f) Ensure proper filing of maintenance certificates after the performance of half yearly maintenance exercises.
g) The environmental hazardous material shall be disposed in line with the provisions of the departmental Asset Disposal Policy.

6.3.6. Incident Reporting

Officials shall be obligated to report instances of violations of this policy.

7. APROVING AUTHORITY

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

8. ACCOUNTABLITIES AND RESPONSIBILITIES

8.1. The Chief Information Officer

The CIO 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.

8.2. The ICT Engineering

The ICT Engineer is responsible for implementation of all ICT infrastructure security controls and maintenance of this policy and advising generally on information security controls.

8.3. Employees and Third-Party Employees

Employees and third-party employees are responsible for complying with this policy.

8.4. The ICT Governance

The ICT Governance function shall be responsible for the continuous assessment of policy implementation and the monitoring of adherence across the Department. It must provide expert advice on information security controls and shall ensure that the Access Management Policy remains robust and effective.

8.5. ICT Steering Committee

The ICT Steering Committee shall be responsible for the strategic oversight of ICT processes. It must ensure continuous alignment between the ICT strategy and the Department's broader business goals. The Committee shall further be tasked with monitoring and directing resource investments to ensure the successful advancement and sustainability of this policy.

8.6. ICT Operational Committee

The ICT Operational Committee shall be accountable for the tactical execution of this policy. It must ensure that the configuration, provisioning, and de-provisioning of access rights comply strictly with the established management intent. The Committee shall oversee the technical application of controls and must ensure the security and functionality of the ICT environment is never compromised.

8.7. Risk Committee

The Risk Committee shall be responsible for identifying, assessing, and monitoring risks associated with the management of user access, integrating access management vulnerabilities into the Department's Enterprise Risk Management (ERM) framework, providing recommendations on the Department's risk appetite, and reviewing the effectiveness of internal controls and audit findings to mitigate the risk of unauthorised access, data breaches, or non-compliance with **POPIA**.

8.8. Member of Executive Council

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

8.9. 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.

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

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

12. POLICY REVIEW

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

13. POLICY RECOMMENDATION AND APPROVAL

Recommended/Not Recommended

Mr. M. Machemba
Head of Department
Eastern Cape Department of Social Development

04/05/2026
Date

Approved/Not Approved

Ms. B. Fanta
Member of the Executive Council
Eastern Cape Department of Social Development

04/05/2026
Date