



Province of the
EASTERN CAPE
COOPERATIVE GOVERNANCE
& TRADITIONAL AFFAIRS

ICT SECURITY POLICY

Departmental Contact Details	
Physical Address	Tyamzashe Building Phalo Avenue Bhisho 5605
Postal Address	Department of Cooperative Governance and Traditional Affairs Private Bag X0035 Bhisho 5605
Document Number	3
Document Name	ICT Security Policy
Custodian	Ms T.M. Luke
Designation	Director: Information Management Services
Component	DGITO
Telephone No.	040 940 7235
Cell Phone No.	076 141 1749
E-mail Address	tswakai.luke@eccogta.gov.za
Date Completed	30 November 2021
Date of Approval	
Date Last Amended	
Date For Next Review	December 2026
Related Policies	ICT Acceptable Use Policy


SIGN OFF

Head of Department

This Policy has been recommended by Mr. AA Fani in my capacity as Head of Department of Department Cooperative Governance and Traditional Affairs.

I am satisfied and concur with the contents of this Policy.

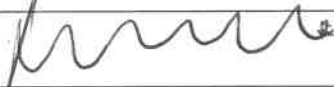
The development of the policy on ICT Security will ensure the Department is able exercise its powers in compliance with the law and guide decision-making in the department.

Signed	
Designation	Mr. AA Fani, Head of Department: Cooperative Governance and Traditional Affairs
Date	07/03/2022

Executive Authority

The Department of Cooperative Governance and Traditional Affairs has an unprecedented opportunity to improve the livelihoods of the people by effectively rendering the many services that it is expected to provide. We have envisaged a Department that has the required capacity to respond adequately to challenges of its people.

I therefore trust that guidance from this ICT Security Policy will contribute to the effective utilisation of the policy by the staff of the Department.

Signed	
Designation	MEC: Honourable XE Nqatha of Cooperative Governance and Traditional Affairs
Date	10/03/2022

1. CONTENTS

1. PREAMBLE 6

2. PURPOSE OF POLICY 6

3. DEFINITIONS 6

4. APPLICATION AND SCOPE 7

5. LEGISLATIVE FRAMEWORK..... 7

6. CONSULTATION PROCESS WITH STAKEHOLDERS 7

7. POLICY PRINCIPLES INHERENT IN THE ICT ACCEPTABLE USE POLICY 8

8. POLICY STATEMENT 8

9. POLICY CONTENT 8

 9.1. ICT RISK ASSESSMENT 8

 9.2. ICT ASSET MANAGEMENT 8

 9.3. SERVER ROOM ACCESS AND ENVIRONMENTAL CONTROLS 9

10. ACCESS CONTROL TO THE NETWORK 10

 10.1. USER ACCESS..... 10

 10.2. LOGICAL ACCESS 10

 10.3. PASSWORD 11

 10.4. MALICIOUS SOFTWARE 12

 10.5. MANAGING NETWORK CONNECTIONS..... 12

 10.6. FIREWALL AND ANTIVIRUS 12

 10.7. WIRELESS SECURITY..... 13

 10.8. WIRED CONNECTION AND CONNECTION POINTS 13

 10.9. ICT SERVICE CONTINUITY MANAGEMENT 13

 10.10. ROLES AND RESPONSIBILITIES 14

 10.11. PRIVILEGED USER ACCESS MANAGEMENT 14

 10.12. ACTIVE DIRECTORY PASSWORD PARAMETER SETTINGS 14

11. REMOTE WORKING PROCEDURE 14

 11.1. REMOTE WORKING SECURITY..... 14

 11.2. REMOTE ACCESS CONTROL 15

 11.3. BACKUP AND MEDIA STORAGE..... 16

12. ENFORCEMENT PROCEDURES 16

13. MONITORING AND EVALUATION OF THE IMPLEMENTATION OF THE POLICY 16

14. COMMUNICATION / EDUCATION OF THE POLICY 16

15. DISPUTE RESOLUTION MECHANISM 16

16. APPROVAL OF THE POLICY 17

17. REVIEW OF THE POLICY 17

18. VERSION CONTROL AND CHANGE HISTORY..... 17

1. PREAMBLE

The Department is committed to protecting its data and systems from threats that arise as a result of its operations conducted via wired and wireless computer networks. The confidentiality, integrity and availability of the information systems, applications, and data stored and transmitted over these networks are critical to the Department’s reputation and success. These information systems and data face threats from a variety of ever-changing sources therefore it is critical that measures are put in place to protect them.

2. PURPOSE OF POLICY

- I. To ensure effective protection and proper usage of the computer systems and its peripherals by all within the Department.
- II. To protect the Department’s information assets from internal and external threats and to safeguard its confidentiality, integrity and availability.
- III. To inform all users of their responsibility to secure and protect all electronic information resources over which they have control.

3. DEFINITIONS

Word/Terminology	Definitions (with examples if required)
DGITO	Departmental Information Technology Office
LAN	Local area network
ICT	Information Communication Technology
DCOGTA/ the Department	Department of Cooperative Governance and Traditional Affairs
Computing devices	Computer hardware, software and accessories owned that can be connected or available via network
Network	Connected devices that make up the Local Area Network
Firewall	A firewall is a set of related programs, located at a network gateway server that protects the resources of a private network from users from other networks.

Word/Terminology	Definitions (with examples if required)
Virus	A piece of code (software) which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or data.
Antivirus	A software designed to detect and destroy computer viruses
Malicious software	Commonly known as malware, is any software that brings harm to a computer system. Malware can be in the form of worms, viruses, trojans, spyware etc.
VPN	Virtual Private Networking
Password	A string of characters that allows access to a computer, interface, or system.

4. APPLICATION AND SCOPE

This policy applies to all employees of the Department of Cooperative Governance and Traditional Affairs including contract workers, interns, seconded workers, service providers.

5. LEGISLATIVE FRAMEWORK

- I. Constitution of the Republic of South Africa, 1996
- II. Minimum Information Security Standards (MISS)
- III. State Information Technology Act (Act no 88 of 1998)
- IV. Electronic Communications Security (Pty) Ltd Act 68 of 2002
- V. Electronic Communications and Transactions Act of 2002
- VI. Electronic Communications Act of 2005
- VII. National Integrated ICT Policy White Paper of 2016
- VIII. National Cybersecurity Policy Framework
- IX. Protection of Personal Information Act (POPI Act) of 2013

6. CONSULTATION PROCESS WITH STAKEHOLDERS

The Departmental Senior Management Service members have been consulted for inputs during the review of this policy.

7. POLICY PRINCIPLES INHERENT IN THE ICT ACCEPTABLE USE POLICY

I. TRANSPARENCY

This policy will be made available to all categories of employees within the Department.

II. PARTICIPATION

All employees of the Department including contract workers, interns, seconded workers, service providers will be required to adhere to the content of this policy.

III. ACCOUNTABILITY

Every employee who has been allocated an ICT asset or resource will be required to account for non-adherence to the provisions of this policy.

8. POLICY STATEMENT

The Department is committed to ensure that computing and communication facilities are used in an effective, efficient, ethical and lawful manner. For this to be achieved it requires commitment and cooperation of all Departmental officials.

9. POLICY CONTENT

9.1. ICT RISK ASSESSMENT

9.1.1. DGITO and Risk Management shall conduct an ICT risk assessment annually.

9.1.2. ICT risk assessment shall identify, quantify, and prioritize risks counter to the measures for risk acceptance and objectives relevant to the Department.

9.2. ICT ASSET MANAGEMENT

9.2.1. All ICT assets shall be recorded in an ICT asset register.

9.2.2. All employees provided with ICT asset shall be held accountable for the protection of the assets under their authority.

9.2.3. ICT asset management procedure shall be developed to monitor and ensure proper management of ICT assets.

9.3. SERVER ROOM ACCESS AND ENVIRONMENTAL CONTROLS

- 9.3.1. Servers shall be in a secure server room that shall be accessed only by authorised ICT employees using biometrics fingerprint system and/or a server room security key. All doors shall be fitted with sensors to detect unauthorized or prolonged opening.
- 9.3.2. Third parties and contractors shall not access the server room without being escorted by a DGITO employee.
- 9.3.3. Third parties and contractors shall upon accessing the server room sign a register stating, amongst other details, the reason for entering the server room.
- 9.3.4. DGITO shall take care and ensure that they prohibit tailgating into restricted areas.
- 9.3.5. Prohibition (No eating, No drinking and No Smoking) and safety signs shall be posted at access points to the Server room.
- 9.3.6. Ear defenders shall be made available and be worn if working in the server room for prolonged periods of time.
- 9.3.7. Smoke and fire detection system shall be fitted and linked to audible alarm.
- 9.3.8. When the fire alarm is triggered at the server room, evacuate immediately to avoid gas inhalation, and normal emergency procedures shall be followed as stipulated in the evacuation procedures.
- 9.3.9. When encountering electrical problems in the server room, a qualified electrical technicians shall be contacted and given access to the electrical system.
- 9.3.10. Air conditioning shall be provided in the server room to deliver enough cooling per rack in accordance with design specification.
- 9.3.11. Temperature and Humidity monitoring devices shall be implemented and set to monitor deviations against baseline set according to standard recommended by GITO.
- 9.3.12. Server room shall be installed with Uninterruptible Power Supply System (UPS). The UPS system should sustain power to all devices for at least 30 minutes to allow all servers to shutdown properly.
- 9.3.13. A reputable service provider to be appointed to undertake maintenance on environmental controls at least four times a year in the server room (e.g. Air conditioning, Fire and Smoke detectors, UPS etc). Certificate for maintenance performed shall be submitted to the Department.

9.3.14. Server room monitoring procedures shall be put in place to monitor on the following issues: -

- 9.3.14.1. Temperature and Humidity alarms.
- 9.3.14.2. Fire and Smoke Detectors.
- 9.3.14.3. UPS malfunctioning
- 9.3.14.4. Air conditioners temperature levels
- 9.3.14.5. Daily monitoring of servers

10. ACCESS CONTROL TO THE NETWORK

10.1. USER ACCESS

- 10.1.1 Only official computing devices shall be connected to the CoGTAs network.
- 10.1.2 Access to the network will be via a secure log-on procedure, designed to minimise the opportunity for unauthorised access.
- 10.1.3 All users to the network will have their own individual user identification and password to control access.
- 10.1.4 A formal, documented user registration and de-registration procedure for access to the network resources will be issued.
- 10.1.5 Departmental line managers and the ICT service desk must approve user access in accordance with this policy and relevant local guidance/processes.
- 10.1.6 Users will only be given sufficient rights to all systems to enable them to perform their job function. User rights will be kept to a minimum at all times.
- 10.1.7 DGITO will control network/server passwords. Service and High privilege account passwords will be assigned by the System Administrator.
- 10.1.8 User access rights will be immediately removed or reviewed for those users who have left the Department or changed positions.

10.2. LOGICAL ACCESS

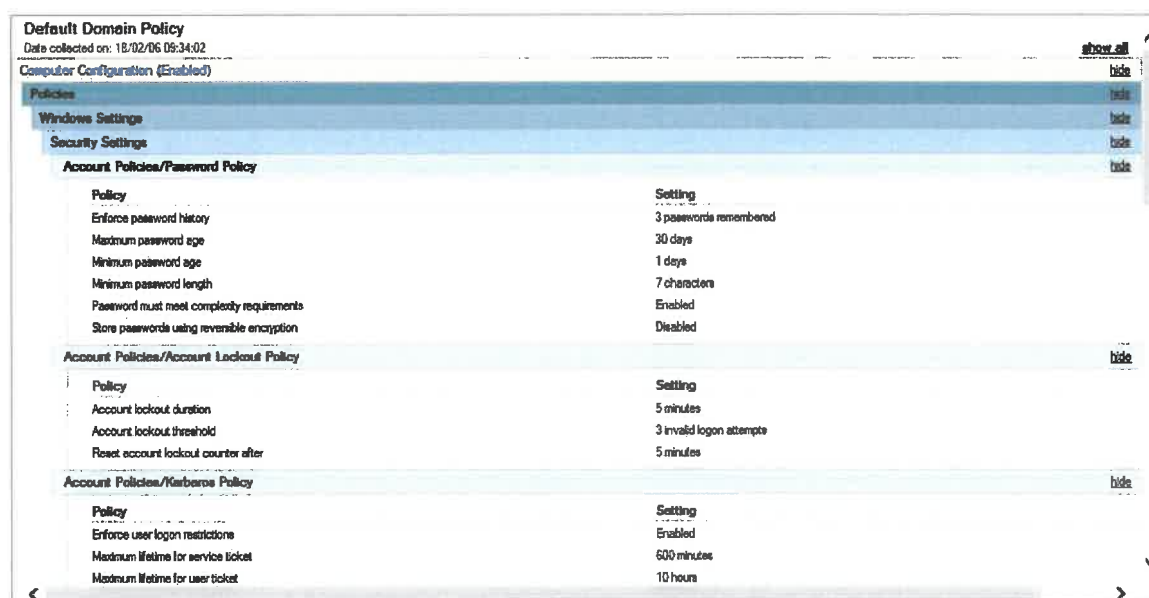
A user account management procedure shall be developed in order to achieve protection of the departmental information systems.

10.3. PASSWORD

The following password policy rules are enforced automatically on Active Directory, they are applicable to all network user accounts:

- I. Password length: 7 characters
- II. Maximum password age: 30 days
- III. Password history: 3 past passwords remembered by system
- IV. Password must meet complexity requirement is enabled (Upper and Lower case and numbers or special characters)
- V. Account lockout threshold will be after 3 invalid logon attempts
- VI. Please refer to the below screen for the detailed password security details on Active Directory (AD)

Figure 1: ACTIVE Directory (AD) Policy configuration



- 10.3.1. Passwords shall be utilised to protect the confidentiality and integrity of the departmental systems
- 10.3.2. Passwords to all systems shall not be shared/divulged; users are not allowed to access other employee’s resources without their knowledge, this shall be classified as an ICT security breach.
- 10.3.3. Users must avoid using guessable passwords such as current month and year, names of own children and anything that can be easily associated
- 10.3.4. All users must change default password to own unique one.
- 10.3.5. New password must not be a simple change of the old password. For example, adding a number at the end.

- 10.3.6. Every reasonable precaution must be taken to ensure that passwords, accounts and data are adequately secured.
- 10.3.7. No attempt should be made to find out another user's password, or to gain access to another user's account.
- 10.3.8. Do not write usernames and passwords on keyboards, walls, monitors, post-it note, table or material. A memorised password is not prone to accidental disclosure.
- 10.3.9. Passwords may not be saved in an electronic document unless the documents are encrypted and the user ensures that the encryption key cannot be accessed.
- 10.3.10. Password must not be sent via email.

10.4. MALICIOUS SOFTWARE

- 10.4.1. Any user who notices unusual behaviour of a computer or system must report it to DGITO helpdesk immediately as this might be as a result of malicious codes such as Virus, Trojans, Worms and Spyware.
- 10.4.2. Autorun for removable drives should be disabled on the group policy to avoid malicious software being installed on computers.
- 10.4.3. On going security vulnerabilities tool must be run for the management and monitoring of security incident.
- 10.4.4. The Patch management procedure should be updated and maintained, in order to manage ICT security controls.
- 10.4.5. DGITO helpdesk contact numbers are 040 940 7244/7442.

10.5. MANAGING NETWORK CONNECTIONS

- 10.5.1. Only authorised entities are allowed access to the Department network. All entry points to the Department network must be reviewed and approved by the DGITO in line with prevailing SITA guidelines.
- 10.5.2. Any inbound/outbound connections between networks, sub-networks, network elements, machines or applications must be such that none of the participants suffer any degradation of security. Security must be maintained such that the purity of a trusted network is not compromised.
- 10.5.3. The creation of a remote access facility must never compromise the security of the Department network or any existing Department system or data.

10.6. FIREWALL AND ANTIVIRUS

- 10.6.1. Only authorized Firewall Administrator(s) shall be permitted to logon to the Firewall hosts. Access to Firewall hosts shall be highly controlled and monitored.
- 10.6.2. All amendments to the Firewall are the responsibility of the authorized Firewall Administrator(s) and must be monitored thoroughly. When there is a necessity for Firewall Rule maintenance or configuration by the service provider, a documented

agreement between the department and the service provider shall be created as an authorizing agreement.

- 10.6.3. At the very least, Firewall shall be configured to use system logging and perform security services. The Firewall shall adequately provide audit capabilities to detect all unauthorized network intrusion activities such as but not limited to attempted network intrusion or any unauthorized traffic. More often, Firewall Administrator(s) shall examine logs and also provide measures to attend to the alerts.
- 10.6.4. DGITO is responsible to ensure implementation of an effective firewall and antivirus security strategy are implemented for the department.
- 10.6.5. DGITO is responsible to ensure that the latest version of antivirus software is installed on all computers.
- 10.6.6. Departmental employees who are field workers are responsible to ensure that their computers are plugged into Departments network for antivirus updates.
- 10.6.7. Staff members are responsible for scanning all media (memory sticks, CDs, external hard drives) before use. Assistance can be requested from an IT technician when necessary.
- 10.6.8. Staff should not attempt to disable or interfere with the virus scanning software.

10.7. WIRELESS SECURITY

- 10.7.1. Proper security controls, such as authentication, logging, and encrypted transmission must be implemented on all wireless devices.
- 10.7.2. A periodic process must be in place to identify and remove rogue access points connected to the COGTA corporate network.
- 10.7.3. Wireless LAN's must be configured to use the most secure encryption and authentication facilities available.
- 10.7.4. DGITO must ensure wireless access point firmware is kept up-to-date.

10.8. WIRED CONNECTION AND CONNECTION POINTS

All network points are to be disabled unless they are actually in use or enabled to allow approved equipment to connect in the near term. Where areas are to be left unoccupied for periods in excess of a few days then network connectivity to the particular area is to be disabled until it is to be occupied again.

10.9. ICT SERVICE CONTINUITY MANAGEMENT

- 10.9.1. ICT Business Continuity and Disaster Recovery plans and procedures shall be established and maintained to facilitate that business processes can continue and be recovered in the event of failures or disasters. These documents shall be developed to minimize the impact of any unforeseen incident in the business functionality and recover critical business operations and application systems within estimated time.

10.9.2. Backup shall be tested on a monthly basis to ensure that there are no flaws.

10.9.3. Backups shall be stored in a physical different location from its origination point of formation.

10.10. ROLES AND RESPONSIBILITIES

The department has two levels of user accounts and table below clarifies their roles

Roles	Responsibilities
Ordinary domain user account	This access is allocated to departmental staff personnel to access resources on the network.
Domain administrator user account	This type of user account is allocated to system administrator to manage network resources such as software installation, system configuration, user permission management, resource allocation

10.11. PRIVILEGED USER ACCESS MANAGEMENT

In order to carry out their responsibilities, administrators need the permissions required to execute such tasks as software installation, system configuration, user permission management, resource allocation, and more.

- Each privileged user has been allocated with username and password
- Sharing of username and password is not allowed
- The default Administrator account has been renamed as to ensure it remains anonymous to an outsider

10.12. ACTIVE DIRECTORY PASSWORD PARAMETER SETTINGS

- The group policy has been configured to lockout password if the user has attempted three times to login and please refer to point 10.3
- The password strength combination should include at least one (1) special character, a capital letter, a number and at small character.

11. REMOTE WORKING PROCEDURE

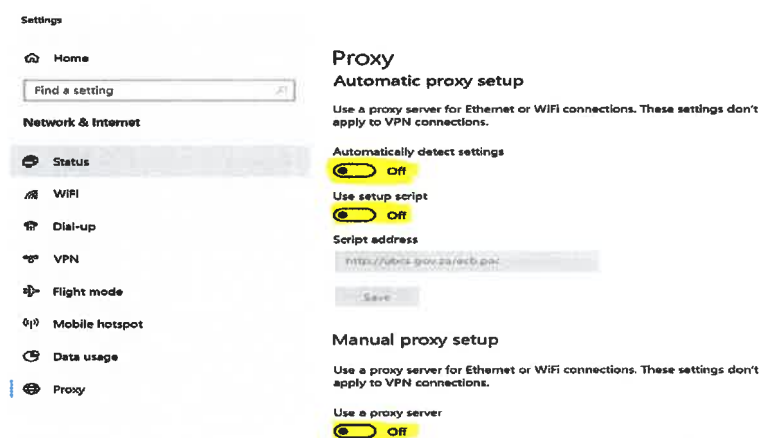
11.1. REMOTE WORKING SECURITY

11.1.1. **Remote Working Privileges** – All employees working at home or at alternative sites must be specifically granted this privilege by the Head of Department.

11.1.2. **Approved Remote Worker Equipment** – All employees working at home or at alternative sites must use the computer allocated by the Department.

- 11.1.3. **Malware Protection Software** – All systems that access the departmental networks remotely must have an anti-malware (anti-virus) package approved by the Department continually running.
- 11.1.4. **Advanced Endpoint Protection** – All systems that access the departmental networks remotely must have an endpoint protection software package installed that protects the system from advances threats.
- 11.1.5. **Setting Date and Time** – All employees working at home or at alternative sites must diligently keep their remote computers’ internal clocks synchronized to the actual date and time.
- 11.1.6. **Changing Proxy settings** - All employees working at home or at alternative sites and connecting to the internet using 3G card or WIFI must ensure that the proxy settings are OFF as per figure 2 below.

Figure 2: Changing proxy settings to OFF whilst using 3G or WIFI



11.2. REMOTE ACCESS CONTROL

- 11.2.1. **Access Control System** – All employees working at home or at alternative sites must not use a remote computer for departmental business activities unless this same computer runs approved active directory access control.
- 11.2.2. **Remote Access to Networks** – All remote access to departmental networks must be made through approved Remote Access points that are controlled by DGITO.
- 11.2.3. **Session Logout** – After a remote worker has completed a remote session with departmental computers, the worker must log off and then disconnect, rather than simply disconnecting. Workers using remote communications facilities must wait until they receive a confirmation of their log off command from the remotely connected departmental servers before they leave the computer they are using.

- 11.2.4. **Screen Positioning** – The display screens for all systems used to handle departmental sensitive information must be positioned such that they cannot be readily viewed by unauthorized persons through a window, over a shoulder, or by similar means.
- 11.2.5. **Sharing Access and Systems Prohibited** – All employees working at home or at alternative sites must not share passwords, or any other access devices or parameters with anyone.
- 11.2.6. **Secure Workspace** – Whenever possible, remote working must be done in a secure environment and must keep sensitive information and mobile devices at their homes to perform their work.
- 11.2.7. **Remote Working Environmental Controls** – Equipment should be located and/or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

11.3. BACKUP AND MEDIA STORAGE

Backup Procedures – Remote workers are responsible for ensuring that their remote systems are backed up on a periodic basis, either automatically through the network or remotely with USB drives or similar equipment.

12. ENFORCEMENT PROCEDURES

- Implementation of group policies

13. MONITORING AND EVALUATION OF THE IMPLEMENTATION OF THE POLICY

DGITO will report any challenges that arise in the implementation of this policy to the ICT Steering Committee.

14. COMMUNICATION / EDUCATION OF THE POLICY

The ICT Security Policy will be communicated to Departmental employees through induction workshops / policy rollout sessions, internal news bulletin and available on the departmental intranet for sharing information.

15. DISPUTE RESOLUTION MECHANISM

In the event of disputes arising out of this policy, such disputes will be dealt with in terms of the grievance procedure and labour legislation applicable in the Public Service.

16. APPROVAL OF THE POLICY

The policy will be approved by Member of Executive Council (MEC) on the recommendation of the Head of Department.

17. REVIEW OF THE POLICY

This policy will be reviewed on every fifth year from the date of approval and/or when there are changes in legislation or the operating environment.

18. VERSION CONTROL AND CHANGE HISTORY

Version Control	Date Effective	Approved By	Amendment
Start from	YYMMDD (the date the policy takes effect)	Contact person – full name & title.	Include any superseded procedures and what the amendment is to the document.
2013	20/12/2013	Mlibo Qhoboshiyane (MEC)	
2016	31/01/2017	F.D Xasa (MEC)	Order has been rearranged to facilitate easy reading. Copied over to updated CoGTA template.
2021		X Nqatha (MEC)	Updated to include remote working security and access control, physical and environmental controls, patch management and password controls