health
Department:
Health
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

Ground Floor, Health Office Park
Private Bag X 2068
MMABATHO

INFORMATION & COMMUNICATION TECHNOLOGY

Tel: +27 (18) 391 4011
Emai: hmetsileng@nwpg.gov.za
www.health.nwpg.gov.za

A long and healthy life for all communities of the North West Province

INFORMATION TECHNOLOGY SECURITY POLICY

JUNE 2023

Author	INFORMATION AND COMMUNICATIONS TECHNOLOGY DIRECTORATE
Review Date	June 2026
Description	This document defines the Department's position on Information Technology Security
Coverage	All employees of the North West Department of Health and all stakeholders.
Policy number	***ICT23/P02/R26***

Table of Contents

1. Introduction

1.1. Information Technology security has come to play an extremely vital role in today's invariably technically fragile business environment. The importance of this fact needs to be clearly highlighted so that adequate measures will be implemented, not only enhancing the department's daily business procedures and transactions, but also to ensure that the much-needed security measures are implemented with an acceptable level of security competency.

1.2. Information takes many forms. It can be stored on computers, transmitted across networks or printed. There are key critical information security components to consider and they are:

a) **Confidentiality** - Protecting sensitive information from unauthorised disclosure or intelligible interception;
b) **Integrity** - Safeguarding the accuracy and completeness of information and computer software;
c) **Availability** - Ensuring that information and services are available when required;

1.3. The North West Department of Health (NWDoH) recognises the value that Information Technology security brings to its effectiveness. This policy addresses how the three IT security components discussed above will be dealt with in the department.

2. Purpose

2.1. The purpose of this policy is to ensure that Information Technology environment and Information Resources are managed in accordance with acceptable industry security standards.

3. Scope

3.1. This policy applies to all staff of the department, partners of the department, contracted service providers, 3rd party organisations and any other person or organisation which uses the department's IT and information resources, be it infrastructure, information, hardware or any other IT resource, intellectual property of the NWDoH, IT Disaster Recovery Planning, IT security administration. This policy further covers all IT resources, that is, networks, internet access, email, hardware, data storage devices, software applications, telephony services, and all other IT resources applicable in the NWDoH domain.

4. Legislative mandate

4.1. Legislative Framework

a) Constitution of the Republic of South Africa, 1996 (Act No 106 of 1996)
b) Public Service Act, 1999;
c) Public Service Regulations 2001 as amended;
d) Public Finance Management Act, 1999 (Act No.1 of 1999);
e) Treasury Regulations issued in terms of PFMA, 1999;
f) Criminal Procedures Act, 1977 (Act No 51 of 1977) as amended.
g) Copyright Act, 1978 (Act No 98 of 1978).
h) Electronic Communication and Transaction Act, 2002 (Act No 25 of 2002).
i) Electronic Communications Security (Pty) Ltd Act, 2002 (Act No 25 of 2002).
j) State Information Technology Agency Act, 1998 (Act No 88 of 1998).
k) National Strategic Intelligence Act, 1994 (Act No 39 of 1994).
l) Protection of Personal Information Act, Act No. 4 of 2013

4.2. Other Policies and Procedures

a) Security Management Policy
b) Information Management Policy
c) Records Management Policy

d) Security and Records Management IT Security Directives
e) SACSA/090/1(4) Communication Security in the RSA
f) Minimum Information Security Standards
g) Managing Electronic Records in Governmental Bodies: Policy, Principles and Requirement

5. IT SECURITY MANAGEMENT

5.1. Information Security Management reflects the Department's commitment to comply with best practice principles to govern and protect the security of sensitive and confidential information. Wherever possible, this policy establishes a balance between the risk of loss of information resources, including data misuse, effort and cost of the security measures. It includes provisions to reduce, as far as feasible, the risk of theft, fraud, destruction, sabotage or other misuses of the Department's information technology resources.

5.2. Administrative information processing, digital telecommunications and related technology are critical business operations of the Department. Inappropriate exposure of sensitive information, loss of data and inappropriate use of computer networks and systems can be minimized by complying with reasonable standards, attending to the proper design and control of information systems and applying sanctions when violations of this Security Policy occur.

5.3. Potential risks associated with IT security

a) Users with higher than necessary levels of access;
b) Workstations not logged off correctly;
c) Shared usernames and passwords;
d) Lack of adherence to procedures;
e) Lack of security awareness;
f) Unauthorised access and computer hacking;
g) Viruses;
h) Dial-in access;

i) Lack of control over changes made to the systems or data;
j) Inadequate Infrastructure and poor maintenance;
k) Public embarrassment and legal consequences of security breach;
l) Fire, water and other liquids;
m) Extreme temperatures;
n) Sabotage;
o) Commercial risks;
p) Unsecure remote access; and
q) External storage devices.

5.4. Users Rights and Responsibilities

5.4.1. Users of IT resources have a right to privacy while engaged in legitimate activity on the Department's IT facilities.

5.4.2. Where such action is taken, users who have data inspected, and are found to be conforming to this policy, have a legitimate expectation that confidentiality will be preserved.

5.4.3. Users responsibilities include:

5.4.3.1. Ensuring that confidentiality and privacy of departmental data is maintained
5.4.3.2. Safekeeping of their usernames and passwords
5.4.3.3. Changing workstation password periodically as required.
5.4.3.4. Ensuring the safety and security of their workstations by logging off or locking it when it is left unattended
5.4.3.5. Ensuring the security and privacy of printouts
5.4.3.6. Compliance with Department's IT Security policy, procedures and controls and other relevant prescripts related to management of IT security.
5.4.3.7. Not using the username or password of other users
5.4.3.8. The safe keeping of IT equipment assigned to them.
5.4.3.9. Using the allocated IT resources only for official departmental duties and/or tasks.

5.5. Department's rights and responsibilities

5.5.1. The Department may inspect, without notice, any data on any computing resource owned by it, including electronic mail and other forms of communication. The approval of the HOD must be obtained before such inspection is done. The inspections of such will be conducted by Central IT(Office of the Premier) as the owners of network infrastructure and internet resources in the North West Province and forward such information to the HOD.

5.5.2. Whilst users have legitimate expectation to privacy in carrying out approved activity on Department's IT resources, the department also has a legitimate right to inspect any data on Department's IT resources to prevent, detect and minimise unacceptable activities on those IT resources. Unacceptable behaviour includes but is not limited to use of departmental assets for personal use; accessing pornographic websites; distribution of pornographic material including child pornography; organised criminal activities; promotion/or perpetuation of racism, sexual discrimination or any other form of discrimination; and any other illegal activities as defined in the South African laws. Unacceptable behaviour also includes storage and distribution of illicit material through government computing resources.

5.5.3. The department reserves the right to access all information and data in its IT facilities for purposes of investigation of any unlawful activities such as fraud, corruption and other suspected criminal activities.

5.5.4. The department reserves the right to copy any data or information contained in its IT facilities and may share such information with any appropriate member of the department's community or law enforcement bodies for purpose of criminal investigations or internal disciplinary hearing.

5.6. Physical Security

5.6.1. All server and network rooms must meet acceptable minimum standards.

5.6.2. Access to the server and network rooms must be logged in a register. This requirement must be fulfilled by all, including, staff, cleaners, technicians, management, visitors, auditors and third-party vendors.

5.6.3. Third-party vendors and internal officials must be accompanied by an IT directorate staff member at all times when accessing the server room.

5.6.4. Maintenance records of IT equipment must be kept safe.

5.6.5. All computer equipment in server rooms and network rooms/cabinets must be connected to an Uninterrupted Power Supply (UPS) device.

5.6.6. The UPS must be tested at least once a year and batteries checked for recommended use dates and physical defects.

5.6.7. A fire detection system must be present in every server and switch room.

5.6.8. Removal of any IT equipment or an IT asset must be accompanied by an assert removal form completed by the remover and approved by the Director Asset Management or Director: Security and Records Management or a delegate official.

5.6.9. Before temporary off site removal of any computer equipment, a computer removal document must be filled in by the user and approved by the Director: Asset Management or Director: Security and Records Management.

5.6.10. All server and switch rooms must be locked at all times when access is not required.

5.7. User Account and Password Management

5.7.1. All systems must have user accounts management procedures.

5.7.1.1. Issuing of Accounts

a) The North West Department of Health shall make decisions regarding access to their respective data or computing environments based on role, assignment and hierarchy in line

with government policies and job requirements. Account setup and modification shall be processed only if approved by the applicant's supervisor on the application form.

Note: Users need to fill in a User Account Management Form.

b) The North West Department of Health shall issue a unique account to each individual authorized to access part of online or offline computing and information resource.

c) Least privileges need to be assigned to individuals to successfully do their duties when creating user accounts or altering functions as per request. Approval of User Account Creation Request should always precede actual User Account Creation.

d) Users' identity must be authenticated before providing them with an account and password details. Acceptable identity documents (Passport, Driver's license, Identity Book/Card). If an automated process is used, then the account holder should be asked to provide several information items that in totality could only be known by the account holder.

e) Passwords for new accounts should not be emailed to remote users unless the email is encrypted or in line with password management policy.

f) The date when the account was issued should be recorded in an audit log.

5.7.1.2. **Managing Accounts**

a) All accounts on Departmental specific systems shall be reviewed at least once a year by the System Administrator to ensure that access and account privileges are commensurate with job function, need-to-know principle, and employment status. The Information Security Officer (ISO) or any individual assigned the role may also conduct periodic reviews for any system connected to the Department of Health network.

b) All guest accounts (for those who are not official members of the North West Department of Health) with access to computing resources of the Department shall contain an expiration of a period not exceeding the approved time of executing the functions and shall be approved by the Director: IT or a delegated official.

c) All guest accounts must be sponsored by the appropriate authorized member of the administrative entity managing the resource.

d) An employee's access to a user account will be changed/modified/ terminated in accordance with the employee's new job functions and requirements by the Network/System Administrator, once the employee has transferred to a different job responsibility or function;

e) All user accounts will be terminated immediately by the Network/System Administrator, upon an employee's departure from the department either by dismissal, transfer, resignation, retirement, death or any other forms of departure. The Network/System Administrator will produce a quarterly report for the Director: IT, providing details regarding the terminated user accounts.

f) The North West Department of Health shall be responsible for the prompt deactivation of accounts when necessary, i.e. accounts for individuals whose employment has been terminated shall be removed/disabled/revoked from any computing system at the end of the individual's employment or when continued access is no longer required; and, the accounts of transferred individuals may require removal/disabling to ensure changes in access privileges are appropriate to the change in job function or location.

g) The Director: ICT or a delegated official shall review all administrator accounts at least four (4) times in a year to monitor activities of all users with administrator accounts. These reviews exclude transversal systems which shall be reviewed in line with their relevant governing documentation such as policies and or Standard operating Procedures.

5.7.1.3. **Departmental Accounts**

a) For access to sensitive information managed by a department, account management should comply with the standards outlined in this policy. In addition, naming conventions must not cause contention with centrally managed email addresses or usernames. Should the potential for contention arise, the applicable system(s) shall not be connected to the campus network until a mutually satisfactory arrangement is reached.

5.7.1.4. **Shared Accounts**

a) Use of shared accounts is not allowed unless when a provision to support the functionality of a process, system, device (such as servers, switchers or routers) or application may be made (e.g., management of file shares). Such exceptions will require documentation which justifies the need for a shared account.
b) Each shared account must have a designated owner who is responsible for the management of access to that account. The owner is also responsible for the above mentioned documentation, which should include a list of individuals who have access to the shared account. The documentation must be available upon request for an audit or a security assessment.
c) All shared accounts must be approved by the Director: IT before such accounts are created.

5.7.1.5. **Password Management**

a) Passwords are an important aspect of computer security. They are a primary defence mechanism on many computer systems.
b) Passwords must not contain the user's entire Account Name value or Full Name value. Both checks are not case sensitive.
c) Password's complexity, length, encryption, use history should conform to the standard set for the specific system SOP.

d) Passwords must never be written down on a piece of paper or displayed in any form.
e) Users must not share passwords with anyone.
f) Users must use different passwords for different systems.
g) Passwords should be changed periodically, the SOP or procedure manual for a particular system will determine the period.

5.8. Data Backup

5.8.1. A full backup must be performed at least once per month.
5.8.2. Daily backups must be performed as incremental backups where necessary.
5.8.3. Backup logs must be checked on a daily basis to ensure successful completion of backups.
5.8.4. Cleaning of backup devices should be performed according to manufacturer's specifications.
5.8.5. Completed backups must be stored off-site.
5.8.6. All backups must be validated and tested at least once monthly.

5.9. Server Security

5.9.1. Access control to the server rooms must be strictly controlled in the following manner.

a) The server rooms must always be locked unless when they are been attended to in any form be it maintenance, any visit or cleaning.

b) The key to the server rooms must be handled by one appointed official and the spare key must be stored off-site. A log book for the key must be kept up to date and all people using the server room must sign for the key when they collect it and when they return it.

5.9.2. An account lockout duration should be configured.

5.10. Virus Protection

5.10.1. All systems must have an anti-virus software prescribed by the Provincial IT or the Department.

5.10.2. Users must scan removable media before use on computers.

5.10.3. The department shall use the centrally procured anti-virus software by Central IT (Office of the Premier). In cases there are challenges with the centrally procured anti-virus software, the department may conduct its own risk assessment and approve use of an internally (departmental) procured anti-virus software.

5.11. Firewalls

5.11.1. All external connections must be protected by firewall managed by Provincial/ Central IT.

5.11.2. Every system-based firewall must be configured with a deny-by-default policy.

5.11.3. Internet access must be controlled by the Provincial IT proxy server.

5.11.4. Authentication to the firewall must be controlled by individual account access and the administrator username and password must be changed and renamed.

5.11.5. User accounts must be assigned with the lowest level of privileges required to perform duties.

5.11.6. System-based firewall software should be patched and updated on a regular basis.

5.11.7. Logging of firewall data should be enabled.

5.11.8. Logs should be reviewed on a weekly basis.

5.11.9. Logs should be archived on a monthly basis.

5.11.10. Configuration logs should be backed up on a monthly basis and after every configuration change.

5.11.11. Administrators should be alerted in the event of possible attacks and in the event of system failure.

5.12. Remote Access Connection

a) Remote access to the department's systems will be provided to selected staff and service providers based on the job they want to do on the network.
b) Remote access will be allowed on the basis of strict controls that reduce the possibility of unauthorised access to the departmental systems and data.
c) Remote access will be controlled by usernames and passwords.
d) Remote access must only be used for activities that are directly related to the department.
e) Remote access to the department's computing resources is considered an extension of the department's network and it's subject to all departmental policies relating to the use of computing facilities.

5.13. Workstation Security

a) Users are not allowed to have administrative access on workstations and laptops.
b) Any services that are not needed must be disabled.
c) All computers must have username and password configured.
d) A lock screen should be activated for all computers.
e) An Administrator account should be enabled in all workstations.
f) All user accounts except the Administrator account should have limited privileges.

5.14. ICT Disaster Recovery Plan

a) The department shall develop and maintain an Information and Communication Technology Disaster Recovery Plan (ICTDRP) to provide for the continued availability of critical services, information and assets if a threat materializes and to provide for appropriate steps and procedures to respond to an emergency situation to ensure the safety of the department's electronic data and information.

5.15. Internet Access and E-Mail Access

5.15.1. Unacceptable Use of Internet and e-mail usage:

a) Email and Internet User Accounts are for the exclusive use of the person to whom they are allocated and must not be used by anyone else.
b) Using profane, obscene, pornographic or other graphic pictures and videos, which may be offensive and / or defamatory to others.
c) Using the Internet to search, access, disseminate, store and retrieve information that is racist, violent, offensive, sexually explicit (sexually explicit content includes e.g. Cartoons, Text Messages as well as Photographs).
d) No user shall engage in/respond to - activities such as political/religious statements, cursing and foul language as well as statements viewed as harassing or discriminative based on race, colour, creed, age, sex, physical disability and/or sexual orientation.
e) Installing commercial software in violation of copyright laws.
f) Allow his or her user account and / or user password to be used by another person unless authorised to do so.
g) Distribute political Party and Campaign information.
h) Use of private email addresses (i.e Yahoo mail, Google Mail etc) is discouraged, however due to availability issues of official email resources, use of private emails will only be permitted when official emails are not available.
i) Official data should not be stored and distributed through unauthorised cloud services (i.e Dropbox, Google Drive, iCloud, One Drive etc)
j) Distribute material for commercial purposes.
k) Transmitting or receiving any data from unauthorised Peer to Peer networks.
l) Engage in any activity that could compromise the security of the North-West Provincial Government's host computer.
m) Accessing "Internet Restricted Sites" without official permission
n) Electronic mailing to groups of people for unofficial purposes (as such, sending large volumes of unsolicited e-mail) is prohibited

o) Forwarding proprietary government and confidential information through the Internet or via Electronic–Mail service, unless duly authorised. Such information should be encrypted if transmitted over the Internet or via Electronic-Mail services.

p) Contravene any laws of the Republic of South Africa through the use of Internet access and Electronic-Mail services.

5.16. Removal of computer generated records

a) Official records should be backed-up and removed from computers before they are formatted or disposed.

b) The hard disks of computers that contain confidential information must be erased at low level and/or destroyed.

c) Information contained in computers that are sent for repairs to service providers must be removed and backed up where possible.

d) In case new equipment is procured; it is the responsibility of the IT technician to ensure that official information is copied to the new equipment before the old equipment is disposed of.

e) The disposal of obsolete hardware must follow the same procedures as the departmental Asset Management Policy.

5.17. Consultants/ Contractors and Third parties

a) Shall sign a non-disclosure of classified information which shall be provided archived by the Security and Records Management Directorate.

b) NWDoH data on consultants'/ service providers' computers should remain the NWDoH data and never be shared outside without authorisation.

6. POLICY IMPLEMENTATION, MONITORING AND EVALUATION

6.1. This policy shall be applicable to the NWDoH domain and all other institutions or individuals that use the Departmental ICT resources.

6.2. The directorate responsible for ICT shall on an annual basis conduct assessment or studies to determine:

a) the shortfalls of the policy in order to inform review
b) whether policy requires review

7. DATE OF IMPLEMENTATION AND REVIEW

7.1. This policy shall be implemented in the NWDoH a month after approval from implementation by the Accounting Officer and the Executive Authority.

7.2. The policy shall be reviewed after three years of implementation or as and when there is a need to do so in order to comply with the national directives or audit requirements or Law as shall be passed by Parliament.

8. *POLICY APPROVAL:*

18/08/2023

Mr. J. De Beer
Chief Director: Strategy and Systems
Date

Recommended/ not recommended

21/08/2023

Mr. O. E. Mongale
Head of Department
Date

Approved/ ~~not approved~~

30/08/2023

HON. MEC. Mr. M. Sambatha
North West Department of Health
Date