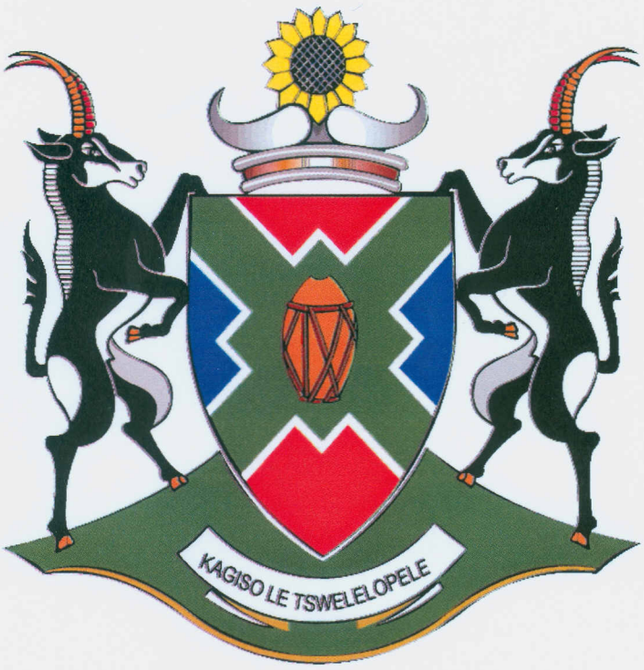
DEPARTMENT OF HUMAN SETTLEMENTS, PUBLIC SAFETY AND LIAISON

(PUBLIC SAFETY BRANCH)



INFORMATION AND COMMUNICATION TECHNOLOGY SECURITY POLICY

(ICTSP - VERSION 1)

TABLE OF CONTENTS

Glossary of Terms

ICT	Information Communication Technology
Dhsps&I	Department of Human Settlements, Public Safety and Liaison
Department	Department of Human Settlements, Public Safety and Liaison(Human Settlements Branch)
COBIT	Control Objectives of Information and related technology
ITIL	Information Technology Infrastructure Library
MISS	Minimum Information Security Standard
MPSS	Minimum Physical Security Standard
CGICTPF	Corporate Governance of ICT Policy Framework
HoD	Head of Department
GITO	Government Information Technology Officer
SLA	Service Level Agreements
NWPG	North West Provincial Government
Sensitive Information	This includes any strategic information of the department, such
SITA	State Information Technology Agency
SSA	State Security Agency
Stakeholders	Auditor General, Provincial Internal Audit, GITO Council, SITA, SSA)
Critical Information	Information is designated as critical information if its unavailability would have a catastrophic adverse impact on the following: • Client or employee life, safety, or health. • Payment to suppliers or employees. • Revenue collection. • Communications.

	• Legal or regulatory.
Official devices	Items provided with permission to access the departmental resources. E.g. Desktop, Laptops etc
Information Systems	A combination of hardware, software, infrastructure and trained personnel organized to facilitate planning, control, coordination, and decision making in an organization.
Information Technology(I.T.)	The study or use of systems (especially computers and telecommunications) for storing, retrieving, and sending information.
User	Employee or any authorized person(s) utilizing departmental ICT equipment
Server	A software program, or the specialised computer on which that program runs, that provides a specific kind of service to client software running on the same computer or other computers on a network..
ISO	International Standard for Organization
SACSA	Special Assistant for Counterinsurgency and Special Activities
Filr	Software by Novell used for backup and remote access of user information
PIA	Provincial Internal Audit
BAS	Basic Accounting System
PERSAL	Personnel Salaries
DMC	Departmental Management Committee

1. Preamble

People, hardware, software, telecommunications, facilities and data form an Information and Communications Technology system that is highly effective and productive. All ICT systems entail the creation of a condition to protect computer hardware, software, and data against incidental and/or deliberate unauthorized changes, destruction, disposal, removal and disclosure. Securing the integrity, confidentiality and availability of the computers and technology systems of the department against threats such as sabotage, unauthorized intrusions, malicious misuse or inadvertent compromise is of paramount importance for the operational effectiveness of all activities of the department.

All users are expected to sign the ICT Policy declaration form (Annexure A), failing which equipments shall not be allocated to them.

2. Regulatory and Guidance Framework

i. Public Service Act (Proclamation No 103 of 1994)
ii. Protection of Information Act 84 of 1982
iii. Promotion of Access to Information Act 2 of 2000
iv. Protection of Personal Information Act of 2013
v. Electronic Communication and Transaction Act 25 of 2000
vi. Regulation of interception of communication and provision of communication-related information Act 70 of 2002
vii. Copyright Act 98 of 1978
viii. Archives and Records service of South Africa Act 43 of 1996
ix. Occupational Health and Safety Act 85 of 1993
x. Public Finance Management Act 1 of 1999 (as amended by Act 29 of 1999)
xi. State Information Technology Agency Act 88 of 1998 (as amended by Act 38 of 2002)
xii. Minimum Information Security Standard
xiii. Minimum Physical security Standard
xiv. National Cyber Security Policy Framework 2012
xv. COBIT 5 Information Security Standards
xvi. ITIL
xvii. ISO 17799
xviii. ISO 27000 series
xix. ISO 38500
xx. SACSA/090/1(4) "Communication Security in the RSA".
xxi. Constitution of the Republic of South Africa (no. 106 of 1996)
xxii. Electronic Communications and Transactions Act (no. 25 of 2002)

xxiii. Communication –related information Act (Act no. 70 of 2002)

xxiv. National Strategic Intelligence Act (Act no. 39 of 1994).

xxv. Provincial Asset management framework

xxvi. CGICTPF

3. Scope of Application

The ICT Security policy is applicable to all employees within the department, third parties and stakeholders utilizing the department's ICT resources and facilities in pursuit of the Department's Goals and Strategic Objectives.

4. Purpose

The purpose of the ICT Policy is to ensure the effective protection and proper usage of the computer systems and its peripherals within the Department. Each employee of the department is responsible for the security and protection of electronic information resources over which he or she has control. Resources to be protected include but are not limited to networks, computers, software, removable media and data. The physical and logical integrity of these resources must be protected against threats such as sabotage, unauthorized intrusions, malicious misuse or inadvertent compromise.

5. Responsibilities

5.1 The Head of Department

5.1.1 The HoD bears the responsibility of overseeing the development, approval, accountability and implementation of the ICT Security Policy.

5.2 Government Information Technology Officer (GITO)

5.2.1 Is responsible for the oversight of development of the ICT policies and strategies, regulations, standards, norms, guidelines, best practices and procedures.

5.2.2 Shall coordinate ICT Security with the ICT Manager.

5.2.3 Shall manage the relationship with all stakeholders that supply Information Technology products and services; this is done by ensuring that all Business Agreements and SLAs are adhered to.

5.2.4 Shall monitor and ensure compliance with relevant ICT regulatory framework and policies.

5.2.5 The GITO shall provide a holistic view of the department's current ICT security posture.

5.3 ICT Manager

5.3.1 Shall ensure that the ICT directorate forsees the implementation of all ICT Security processes in the department by the Security Manager.

5.3.2 Shall ensure that the ICT Security Policy conforms with the Information Security Plan.

5.3.3 In consultation with the GITO shall recommend all ICT projects of the department to the HoD.

5.3.4 In consultation with MISS shall ensure that all ICT service providers undergo all security procedures before providing services to the department.

5.3.5 Shall identify ICT risks.

5.3.6 Shall provide recommendations on remedial actions to be taken to solve all ICT risks faced by the department.

5.3.7 Shall ensure that ICT Directorate complies with the Risk Management Policy.

5.4 Internal Audit

5.4.1 NWPG internal Audit shall audit all ICT Compliance within the department.

5.4.2 NWPG internal Audit shall assist ICT Directorate in ensuring that recommendations provided from the audit findings are implemented correctly.

5.5 Security Services

5.5.1 Shall ensure that all ICT physical security breaches are reported to the ICT Directorate.

5.5.2 Shall in conjunction with the ICT Directorate ensure that the Information Security Policy is implemented and complied with.

5.5.3 Shall ensure the screening of all ICT service providers.

5.5.4 Shall in conjunction with ICT Directorate be responsible for physical protection of all ICT assets of the department.

5.5.5 Shall ensure that all employees having access to business application systems are vetted.

5.5.6 Shall in conjunction with Asset Management ensure that employees of the department are provided with approved movement of ICT assets; {see annexure B for movement of ICT asset}.

5.5.7 It is the responsibility of Security Services to ensure that the department's environment is secured from any internal and external threats.

6. ICT Security Risk Assessment

6.1.1 ICT Directorate and Security services, shall conduct ICT Security Risk Assessments bi annually.

6.1.2 ICT Security Risk Assessment shall assist in identifying the ICT security risks and estimating the magnitude of the risks identified.

6.1.3 ICT Security Risk Assessment shall be conducted in compliance with the Security Management Policy.

7. Third Parties and Contractors

7.1.1 All ICT Directorate third parties and contactors shall be screened/vetted by Security Services before provided with access to any ICT resources.

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

7.1.3 Shall not be provided with access to the sensitive information unless security clearance is provided to Security Services.

7.1.4 SLA's shall be signed by and between the department and Third parties and contractors before providing any ICT services to the department.

7.1.5 Shall be accompanied at all times by ICT Directorate members when providing any services.

7.1.6 Shall not be provided with logical access to any critical information systems of the department; logical access shall be provided only with an approved authorization from HoD, GITO and ICT Chief Director; {see annexure C: Third party Logical access Authorization}

7.1.7 During the ICT Risk Assessment, third parties and contractors shall be covered to identify as to what threats they impose to the department.

8. Asset management

8.1. All ICT equipments shall be recorded and /or tagged with an asset tag.

8.2. ICT asset register shall have the following description:

(a) Value of the asset

(b) Asset owner

(c) Location of asset

(d) Date of acquisition

8.3. All employees provided with ICT equipment shall ensure that such assets are provided with protection from damage and theft; (this to be included in the Acceptable Use of ICT asset).

8.4. Employees not reporting any damage and theft of allocated ICT equipment shall bear the responsibility and the losses shall be recovered from them.

8.5. This shall be done in compliance with the Asset Management Policy.

9. Server room

9.1.1. Servers shall be located in a secure server room that shall be accessed only by authorised ICT employees.

9.1.2. Third parties and contractors shall not access server rooms without any escort from the ICT directorate employees.

9.1.3. Servers shall be accessed only by authorised owners.

9.1.4. Server room shall be designed in accordance with the NWPG Server Room specifications.

10. Patch rooms /cabinets

10.1 Patch rooms /cabinets shall house network Routers and Switches that connect departments to NWPG network resources.

10.2 All ICT Patch rooms/cabinets shall be protected from unauthorised personnel. Departments with ICT Patch rooms/cabinets shall ensure that ICT equipments are provided with minimal security as prescribed in the NWPG Patch Room specifications.

10.3 Access to Patch rooms/cabinets and Server rooms shall be in accordance with the Patch Room and Server Room procedure and guideline.

11. Desktop Security

11.1.1 All desktops provided to employees shall be allocated in accordance with the employee's job description.

11.1.2 Employees shall be given least privileges in desktop operating systems.

11.1.3 Employees shall ensure that they only utilise the equipment for official purposes.

11.1.4 Employees shall only have logical access to their allocated desktop.

11.1.5 No employee, except ICT personnel is allowed to open desktops.

11.1.6 Desktops shall be marked with security cable tie in order to identify if there has been physical temper to the asset.

11.1.7 No desktops shall be removed from the department's premises without authorisation of Asset Management.

12 Mobile Devices

Mobile devices herein refer to official laptops and official tablets

12.1 Official mobile devices shall be issued to employees in accordance with the SCM and ICT policies.

12.2 All employees issued with official laptops shall ensure that they are also provided with security cables.

12.3 Securing of mobile devices is the sole responsibility of the employee issued with such a device.

12.4. Official laptops shall be carried along with the Approval to remove mobile devices, which shall be signed by the employee's immediate supervisor (See Annexure D); Should employees be stopped by SAPS members during stop and searches routines, employees with official removable devices shall provide the SAPS members with Approval to remove mobile devices.

12.4.1. Failure to comply with the stop and searches and not issue Approval to remove mobile devices letter, shall be taken as Theft of government asset.

12.4.2. It is the responsibility of the employee to ensure that such letter is in their possession at all times.

13 Removable devices

Removable devices herein refers to USB Flash Drives, Compact and DVD discs, external Hard-drive and any other removable media storage devices.

13.1 Official removable devices are defined as documents as stipulated in the MISS and the Protection of Information Act 85 of 1985.

13.2 Shall be issued to employees according to their job descriptions.

13.3 All removable devices shall be requested from the ICT Directorate.

13.4 Removable devices that shall be utilised to store classified information shall be installed. with an encryption system and users shall be trained as how to use such encryption system.

13.5 Encryption systems to be utilised shall be an approved system by the GITO and ICT Manager.

13.6 Official removable devices shall be locked away in accordance with the Information Security Policy and MISS.

13.7 Any loss of Removable devices shall be reported to the ICT directorate and to the Security Services.

14 Network Security

14.1.1 Only official desktops and mobile devices shall be connected to the NWPG network.

14.1.2 The department shall not implement any wireless network without consulting the NWPG

14.1.3 ICT Directorate Chief Director.

14.1.4 The Department shall be provided with network security procedures and guidelines by NWPG ICT directorate.

15. Logical Access

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

16. Password

16.1.1 Passwords shall be utilised to protect the confidentiality and integrity of the departmental systems.

16.1.2 Passwords to all systems shall not be shared; users who access other employee's resources without authorisation from ICT directorate shall be classified as an ICT security breach.

16.1.3 Employees shall familiarize themselves with the IT Password Policy.

14. Remote Access

14.1 Remote Access to operational systems is prohibited; operational systems include amongst others: BAS, Persal and Walker Systems.

14.2.1. The following are approved network resources that shall be allowed to be accessed utilising the internet:

(a) Remedy Online

(b) GroupWise

(c) Filr

15. Internet and Email

15.1.1 Internet and Email shall be accessed by utilising user's credentials.

15.1.2 Internet and Email access granted to employees shall not be abused and shall be utilised only for work related purposes.

15.1.3 Uploading government information in free cloud services is prohibited.

15.1.4 Downloading of pirated software and files is prohibited and employees caught doing so shall be warned for abusing government resources.

15.1.5 Employees shall sign Acceptable Usage of Internet and Email.

15.1.6 The above shall be in accordance with the Internet and Email policy.

16. BAS, Persal and Walker

16.1.1. Only approved employees shall be provided with logical access to these systems.

16.1.2. System administrators shall ensure that passwords of these systems are changed every month.

16.1.3. System administrators shall review system users quarterly and review all logs created in the systems

16.1.4. All systems breaches shall be reported to the Systems Administrator and Security Services.

16.1.5. All systems policies and procedures shall be regularly reviewed by system administrators in conjunction with ICT directorate.

17. Malicious Software

17.1. Malicious Software (Virus, Trojans, Worms and Spyware) shall be reported by the employee once identified in the system.

This should be done by:

(a) Contacting the IT helpdesk to report the incident;

(b) IT technician shall assist the user to remove the Malicious Software;

(c) Network Administrator shall ensure that Antivirus installed in systems is setup to scan desktops and mobile devices daily.

17.2. Knowledge base shall be utilised in order to keep record of types of Malwares the department has faced.

17.3. Employees are prohibited from installing unauthorised software.

18. Firewall and Antivirus

18.1.1 It is the responsibility of NWPG IT and the department's ICT manager to ensure the implementation of an effective firewall and virus security strategy for the department.

18.1.2 It is the responsibility of the IT section of the department to ensure that the latest version of antivirus software is installed on all computing devices.

18.1.3 Remote users and users of portable computers should ensure that computers are plugged into Departments network at least twice a week for antivirus updates.

18.1.4 Staff members are responsible for scanning all media (e.g. memory sticks, CDs, external hard drives) before use. Assistance can be requested from an IT technician where necessary.

18.1.5 On detection of a virus, the staff member should notify the ICT section for assistance immediately.

18.6. Staff should not attempt to disable or interfere with the virus scanning software.

19. Incident Management

19.1 All the departmental ICT incidents shall be reported to the central ICT Directorate Helpdesk.

19.2 Remedy System shall be the tool to be used for logging ICT incidents.

19.3 ICT incidents shall be prioritized according to the impact they have on the NWPG network and critical systems.

19.4 An incident response team shall be established in order to recover NWPG downtime; the NWPG ICT incident response team shall include ICT technicians and management.

19.5 Incident management operational procedure and guidelines shall be developed and implemented.

20. Information system acquisition, development and maintenance

20.1. All Information system acquisition shall be procured in line with the SITA procurement procedure.

20.2 Failure to procure Information Systems without following the SITA procurement procedure shall constitute non-compliance with DPSA regulations.

20.3 Should the department utilise a Service Provider to develop an Information System for the department, an SLA shall be signed by and between the Service Provider and the department.

20.4 Security requirements of the Information System must be stated by the department.

20.5 The SLA shall state that the department owns the right of the Information System developed by the service provider, this in line with Copyright Act.

20.6 Skills transfer of the development of the Information System shall also be part of the SLA.

20.7 All acquired Information System shall be tested before being deployed into the live network.

20.8 Information Systems acquired or developed should protect the confidentiality and integrity of the departmental systems.

21. ICT Disaster Recovery Plan

21.1 Information Backups

21.1.1 By default, Central IT has allocated 2,5Gb of disk space for backup on filr server done automatically on a daily basis.

21.1.2 It is the responsibility of the IT section to install filr on all departmental computers.

21.1.3 Users who need filr should contact IT technicians for installation.

21.1.4 Only work related information shall be backed up by the filr server.

21.1.5 Users of laptops should ensure that laptops are connected to the network on regular basis in order for filr to be backed up.

21.1.6 Where the need arises, the IT section shall provide officials with removable devices for the storage of work related information.

21.2 Backup of department's servers

21.2.1 Backups of the systems database shall be done daily on the Server via an automated process available in the operating system.

21.2.2 Access to backups must be done in writing, signed and approved by the head of the Department.

21.2.3 Log files to be maintained on server confirming backup.

21.2.4 Bi-weekly backups of the database and log files shall be done on tapes.

21.2.5 Backups shall be collected weekly on Fridays by IT and handed over to Security Services section.

21.2.6 A register for the maintenance and management of backups to be maintained Register shall include the following:

a. Identification of Backup (ServerName_YYYY/MM/DD);
b. Name of official who made the backup, Signature and Date;
c. Verification of backup(Name of Official, Signature and Date);

d. Random / Scheduled testing and restore of selected backup (Name of Official, Signature and Date, comment = successful or not);
e. handover of backup to IT (Name of Official, Signature and Date);
f. Hand over from IT to MISS section (Name of Official, Signature and Date);
g. Provision for Monthly Sign off of Register By Accounting Officer or delegated Official;
h. Testing of backups shall be done monthly by departmental system administrators;
i. Backup shall be stored in a secured place by the Security Services Manager.

22. ICT Continuity Plan

22.1 ICT Continuity Plan shall be developed and shall be in-line with the departmental business continuity plan.

22.2 Shall identify critical business information systems that should be prioritised.

22.3 ICT Continuity plan shall be endorsed by the DMC.

22.4 Shall provide with details of alternative ICT Data centre to continue providing ICT services to the department.

22.5 Shall ensure that an ICT disaster recovery team is established.

22.6 Shall provide estimated time to recover all systems to be back online.

23 Security Awareness

23.1 ICT directorate in conjunction with Security Services shall conduct Security awareness campaigns.

23.2 A security awareness plan shall be developed by both ICT directorate and Security Services.

23.3 The awareness program shall make employees of the department aware of internal security policies.

23.4 Security awareness shall be presented in a form of face to face engagement, posters, newsletters and utilising the intranet.

23.5 All directorates shall attend security awareness presentations once invited, failure to attend such awareness shall result in non-compliance of this policy.

24. Compliance

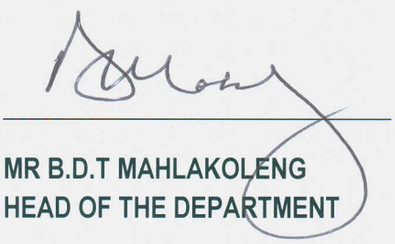
Any disciplinary action arising from non-compliance with this policy, procedures and guidelines shall be dealt with in accordance with Public service disciplinary code and procedures.

25. Review

This policy shall be reviewed annually depending upon the new developments that have been introduced within the Department.

26. Approval

This policy shall come into operation from the effective date i.e. the date upon which it has been signed off and approved by the Accounting Officer.



MR B.D.T MAHLAKOLENG
HEAD OF THE DEPARTMENT

29/02/2024

DATE

ICT SECURITY POLICY DECLARATION FORM

Annexure A

I, (name and surname) _____ of (Persal no) _____ have read the Departmental ICT Security Policy and I fully understand the terms and conditions and agree to abide by it.

The sharing, disclosure of passwords is an offence in terms of Section 3 and 4 of the Protection of Information Act. As the user / applicant, I understand and will refrain from engaging in any practices that could jeopardise the security of any Government system. I am accountable and fully responsible for ensuring that my user password is changed regularly, this includes immediately on receipt of my NEW USER ID, to change my default password.

I understand that any violation of this policy may lead to me being liable for the costs of damage or theft of any ICT equipment in my possession. I therefore undertake to take proper care of any Departmental ICT equipment, software, data or peripheral(s) allocated to me.

_____ _____

Signature of User Date

_____

IT Unit staff member as Witness

ICT ASSET MOVEMENT FORM

Annexure B

Purpose of Movement:

Current Location / User information		New Location / User Information	
Office Number		Office Number	
Name of building		Name of building	
Head/Regional/District Office		Head/Regional/District Office	
Asset User		Asset User	
Asset Controller		Asset Controller	

No	Asset Bar Code #	Room Bar Code #	Asset serial Number	Asset Description	Condition of Asset
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					
9.					
10.					

Movement of ICT Assets Sign Off			
Designation	Name	Signature	Date
Asset Holder			
Asset Receiver			
ICT Personnel			

Department Stamp

LOGICAL ACCESS FORM

ANNEXURE C

ICT Manager			
Asset Manager			

Applicant's Personal Details:	
First Name:	**Surname:**
ID. No.:	**Email:**
Phone No.	**Fax No.:**
Company:	**Section:**
Location:	**User ID/Profile**

Put a tick where applicable:

New User ID		Reset User ID		Reset Password		Request for reports	Install Cables	
		Specify Application below:		Specify Application below:		Specify Reports	Specify Location below:	

If not listed above, kindly describe your request in detail:
E.g. for what system / application, what reports, location of NW cables and points, duration of access, date and time.

Applicant:

Signature: _____ Date: _____

Department Stamp

Duly authorised by Head of the Department

Initials: _____ Surname: _____

Signature: _____ Date: _____

dhsps&I

Department:

Human Settlements, Public Safety & Liaison

North West Provincial Government

3366 Besemmer str Telkom building

Industrial site Mafikeng, 2745

NWDC cnr. . University Drive

STRATEGIC SUPPORT SERVICES

Safety House31-34 Molopo Road
Mafikeng, 2745
P/Bag X 19 Mmabatho 2735

Tel: +27 (18) 381 9104/9132
Fax: +27 (18) 381 9123

ASSET MOVEMENT AUTHORIZATION FORM

ANNEXURE D

I, (Name and Surname) _____ Persal no.: _____ from Department of _____ have been authorized to carry the ICT Asset (description) _____ outside the department's premises, Serial Number _____ and I agree to take full responsibility of this ICT Asset. I fully understand the terms and conditions as stipulated in the ICT Security Policy and agree to abide by it.

Applicant:

Signature: _____ Date: _____

Department Stamp

Duly authorised by:ICT Manager

Initials: _____ Surname: _____

Signature: _____ Date: _____