dcstm

Department:
Community Safety and Transport Management
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF COMMUNITY SAFETY AND TRANSPORT MANAGEMENT

INFORMATION COMMUNICATION TECHNOLOGY SECURITY POLICY

ICTSP VERSION 1.5

Document Details

Author	Directorate Information Communication Technology
Department	Community Safety and Transport Management
Division Name	ICT Management
Document Name	Information Communication Technology Security Policy
Sensitivity	Internal Use Only
Effective Date	<Date of Accounting Officer's signature>
Created Date	01-04-2013
Version Date	<Date of Accounting Officer's signature>
Version	ICTSP-VERSION 1.5

Change Record

Modified Date	Author	Version	Description of Changes
26-11-2012	Directorate Information Communication Technology	1	Original Security Document
01–04 -2013	Directorate Information Communication Technology	1	Compliance to DPSA requirements
26-09-2014	Directorate Information Communication Technology	1.1	Departmental Business Change
31-03-2016	Directorate Information Communication Technology	1.2	Annual Review
31-03-2018	Directorate Information Communication Technology	1.3	Annual Review
30-04-2021	Directorate Information Communication Technology	1.4	Review
	Directorate Information Communication Technology	1.5	Align to the directive on Public Service Information Security

Stakeholder Sign–Off

Name	Position	Signature	Date
Mr O. Gabonnwe	Departmental Information Technology Officer		29/11/23
Ms K. Phatudi	Governance Champion		29/11/23
Ms F. Nchoe	Chairperson: ICT Steering Committee		29/11/23
Ms K. Phatudi	Chairperson: ICT Strategic Committee		29/11/23
Ms M.G. Mothibedi	Departmental Chief Risk Officer		29/11/23
Mr M. Mogatusi	Acting Director Legal Services		29/11/23

Records Management Sign–Off

Name	Position	Signature	Date
Mr E. Khuto	Deputy Director Records Management		06/12/2023

TABLE OF CONTENTS

Glossary of Terms

CGICTPF	Corporate Governance of ICT Policy Framework
Classified Information	Means sensitive information which, in the national interest, is held by, produced in, or under the control of the State or which concerns the State, and which must, because of its sensitive nature, be exempted from disclosure in terms of the Protection of Personal Information Act, 2013
Contractors	A person or business which provides goods or services to the Department
Compromise	Means the unauthorised disclosure/exposure or loss of sensitive or classified information or exposure of sensitive operations, people, or places, whether by design or through negligence.
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 Users. • Revenue collection. • Communications. • Legal or regulatory.
DCS&TM	Department of Community Safety and Transport Management
DISO	Departmental Information Security Officer
DITO	Department Information Technology Officer
GITO	Government Information Technology Officer
HoD	Head of Department

Incident	An adverse event in an information system and/or network or the threat of the occurrence of such an event.
ICT Assets	Computers, communications facilities, networks, data, and encryption keys that may be stored, processed, retrieved, or transmitted by them. This includes programs, specifications, and procedures for the operation, use, and maintenance. All such assets are the property of the department and should be protected according to the policies.
ICT	means all aspects of technology that are used to manage an support the efficient gathering, processing, storing, and dissemination of information (Information Communication Technology).
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.
ISO	International Organization for Standardization
Logical Access	user based authenticated access to application systems and the data that is processed
MISS	Means the Minimum Information Security Standard which is a national government policy document on information security standards that must be maintained by all departments
Mobile Devices	Mobile devices herein refer to official laptops tablets, mobile projector, mobile printers
MPSS	Minimum Physical Security Standard
NWPG	North West Provincial Government
Official devices	Items provided with permission to access the departmental

	resources. E.g. Desktop, Laptops etc
Remote Access	Distanced away from the NWPG server farm, Isolated network (3G e.t.c), network inaccessible areas
SACSA	Special Assistant for Counterinsurgency and Special Activities
SSA	State Security Agency
Sensitive Information	This includes any strategic information of the department, such
SLA	Service Level Agreements
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.
Third Parties *(Do not include AG, Internal Audit)*	Any and all stakeholders or service providers who are not employed by the department but are operating in the Departmental environment
Trusted entities	Means ICT service providers rendering a service to a government department
User	Employee utilising ICT equipment

1. Introduction

Information Communication Technology (ICT) system is made up of people, hardware, software, telecommunications, facilities and data. 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.

2. Purpose

The purpose of this 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.

3. 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. National Archives and Record Services 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 (No 88 of 1998 as amended by Act 38 of 2002)
xii. Minimum Information Security Standard (MISS) of 1996
xiii. Minimum Physical Security Standard

xiv. National Cyber Security Policy Framework 2012
xv. International Organisation for Standardization (ISO) 17799
xvi. International Organisation for Standardization (ISO) 27000 series
xvii. International Organisation for Standardization (ISO) 38500
xviii. Constitution of the Republic of South Africa, 1996 (Act no. 108 of 1996)
xix. Electronic Communications and Transactions A (no. 25 of 2002)
xx. Communication – related Information Act (no. 70 of 2002)
xxi. National Strategic Intelligence Act (no. 39 of 1994)
xxii. Provincial Asset Management Framework
xxiii. Corporate Governance of Information Communication Technology Policy Framework (CGICTPF)

4. Scope and Application

This ICT Security Policy is applicable to all Users in the department, third parties and contractors utilising the department's ICT resources and facilities in pursuit of the Department's Goals and Strategic Objectives.

5. Roles and responsibilities

5.1 Head of Department

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

5.2 Departmental Information Technology Officer (DITO):

5.2.1 ensure the confidentiality, integrity and availability of ICT systems within the ICT environment;

5.2.2 oversee the development of the ICT policies and strategies, regulations, standards, norms, guidelines, best practices and procedures;

5.2.3 coordinate ICT Security management activities within ICT;

5.2.4 manage 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.

5.2.5 monitor and ensure compliance with relevant ICT regulatory framework and policies.

5.2.6 provide a holistic view of the department's current ICT security posture.

5.3 Departmental Information Security Officer (DISO)

Shall be accountable to the Departmental Information Technology Officer (DITO) for matters related to information security.

5.4 Provincial Internal Audit:

Provincial Internal Audit shall provide professional advisory services to the Departmental ICT.

5.5 ICT Steering Committee

Shall function as the Information security forum.

6. Management of ICT related risk

6.1 The Department shall conduct ICT Security Risk Assessment on annual basis in compliance with the *Departmental Enterprise Risk Management Policy.*

6.2 The department shall ensure that ICT-related business risks are identified during the planning cycle and document such risks on a risk register.

7. Third Parties and Contractors

7.1 ICT component third parties and contactors shall be screened / vetted by Security and Facilities Management, or an oath of secrecy shall be signed before provided with access to any ICT resources;

7.2 Shall sign a non-disclosure of classified information which will be provided and archived by the Security and Facilities Management Component;

7.3 Shall not be provided with access to the sensitive information unless security clearance is provided to Security and Facilities Management;

7.4 Service Level Agreements (SLA's) between the Department and Third parties and contractors shall be entered into in order to manage services prior to rendering services to the department;

7.5 Shall be accompanied at all times by ICT Component members when providing any services.

7.6 External ICT consultants, computer security response teams, contractors, or temporary staff who require access to the provincial network must seek authorization in line with the governance arrangements.

7.7 As part of an outsourcing contract procedure, a risk assessment shall be carried out under the guidance of DISO to determine the security implications and security control requirements.

7.8 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; *see annexure D: ICT Logical Access Authorization.*

8. ICT Asset Management

8.1 All ICT equipment shall be recorded and /or tagged with an asset tag according to their classification.

8.2 A register of all ICT Assets shall be kept containing a minimum of the following description:

(a) Value of the asset

(b) Asset owner

(c) Location of asset

(d) Date of acquisition

8.3 It is the responsibility of users provided with ICT equipment to ensure that such assets are protected from damage and theft;

8.4 It is the responsibility of users to ensure that the ICT resources allocated to them are in good working condition.

8.5 Departmental information shall be stored /saved on Departmental computing resources.

8.6 Users are not allowed to possess similar items performing the same function e.g. Laptop/Desktop except in circumstances that are unavoidable. In instances where the official is forced by circumstances to possess similar items performing the same function, authorization shall be granted by the Accounting Officer.

8.7 ICT asset(s) shall be managed in a manner which is compliant to the Departmental Asset Management Policy.

8.8 Hard drive(s) shall be formatted prior to disposal.

8.9 Movement of ICT assets shall be controlled in conjunction with Asset Management and ICT, to ensure that the process is managed properly through the usage of the appropriate form i.e. *annexure B for movement of ICT asset and ICT Allocation form to declare that the computing resources received were in good working condition.*

8.10 In the event, the equipment is reallocated to a different user*, the ICT Reallocation Form (Annexure C)* shall be utilised to manage the process.

8.11 All losses or theft of computing resources must be treated as a security breach and to be reported to SAPS within 24 hours after acknowledgement. Subsequent to that, a report must be forwarded to Loss Control Committee through asset management office / Security and Facilities Management Unit.

8.12 Departmental Human Resources management component shall notify the asset controller and ICT of any resignation/ transfer /termination of employment to identify the computing resources in possession of the official and terminate or deactivate system access/ credentials.

8.13 Departmental Human Resources Management shall ensure that there is a skills transfer plan/ succession plan for system users.

9. Desktop Security

9.1 Computing resources shall be allocated to Users based on their job requirements.

9.2 Users access to desktop operating systems functions shall be limited.

9.3 Users shall ensure that they only utilise the computing resources for official work only.

9.4 Users shall only have logical access to their allocated desktop.

9.5 Users are not allowed to physically open computing equipment.

9.6 Only ICT personnel are allowed to open computing equipment. No computing equipment which is under warranty shall be opened.

9.7 No desktops shall be removed from Departmental premises without authorisation of Asset Management

10. Mobile Devices

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

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

11. Removable Devices

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

11.1 Official removable devices are defined as documents as stipulated in the MISS and the Protection of Information Act 84 of 1982.

11.2 Removable devices shall be issued to Users according to their job demand.

11.3 All removable devices shall be requested from Supply Chain Management Directorate.

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

11.5 Any loss of Removable devices shall be reported to the Departmental Loss Control Committee and to the Asset Management / Security and Facilities Management.

12. Network Security

12.1 Only official desktop and mobile devices shall be connected to the NWPG network.

12.2 The Department shall not implement any wireless network without consulting Office of the Premier IT; should IT manager fail to comply he/she will be held accountable on any security breach that may occur on such wireless network.

12.3 The Department shall be provided with network security procedures and guidelines by Office of the Premier- IT.

13. Protection of information Security devices

Only trusted entities shall be allowed full access to the provincial network. All entry points to the provincial network shall be reviewed and approved by the GITO.

14. Removal of classified documents from premises

a) A destruction certificate shall be issued to the Director of the programme.
b) Retention schedules shall be developed and implemented.
c) Records shall be available to the entire department or only designated part of the department, based on the user's access permissions.
d) Records shall be retained for a period as determined by legislation or best practices.

15. Disposal of media

15.1 The destruction of storage devices shall be conducted by trained and authorized personnel. Safety and special disposition must be identified and addressed before conducting any media destruction.

15.2 The disposal of removable media shall be performed in such a manner that the data is not recoverable.

16. Vulnerability Management

16.1 Vulnerability assessment is the responsibility of Office of the Premier IT as the custodian of the network infrastructure.

16.2 Office of the Premier IT shall ensure that the network infrastructure is kept up to-date and is running the latest and stable software versions.

16.3 The Department shall ensure that Operating System updates and application updates shall be performed at least once a month or more regularly through patch management.

16.4 Vulnerability scans and vulnerability remediation shall be performed bi-annually, through a vulnerability management process.

17. Logical Access

The approved ICT user account management policy is in place to ensure protection of data in the departmental information systems and to regulate access to Departmental Systems. Access to Departmental virtual meeting shall be granted to officials who appear in the list of participants only.

18. Access Control Management

18.1 Formal access granting, access review, and access revoking processes are established and maintained. The above ensure that users have access only to:

I. Their own files and data;

II. Publicly available files;

III. And /or files that they have been authorised to access.

18.2 Systems requiring protection against unauthorised access have the allocation of privileges controlled through a formal authorization process and a record of all privileges allocated must be maintained.

18.3 Login privileges or access allocated to users on a need-to-use and event-by-event basis shall be authorized by the Accounting Officer or delegated i.e. the minimum access required to perform the role.

18.4 Departmental System and technical support staff shall align to a clear separation of functions (such as system administrators vs regular users) to prevent unauthorized access and function from being performed.

18.5 Privileged accounts (ICT Admin) shall not be used for day-to-day use such as reading emails or accessing the internet.

18.6 User access rights shall be reviewed and re-allocated when an employee moves from one business unit to another within a department.

19. Password Management

19.1 Password Construction

a) Password should be eight (8) to twelve characters in length;

b) Passwords must not consist of repeated character strings (e.g.Odu1111);

c) Passwords must not consist of sequential numbers or characters (e.g. 123456);

d) Passwords must be alphanumeric;

e) Users must be discouraged from using default passwords;

f) Passwords must not mirror the corresponding user id;

g) Password must be changed frequently, at least every ninety (90) days.

19.2 Password rules

a) Passwords must be kept a secret;

b) Do not write down your password, particularly anywhere near your computer or file it in a box file with the word "password" written on it;

c) Do not tell or give out your passwords to other people, even for a very good reason.

d) Do not display your password on the monitor.

e) Do not send your password via email.

f) Avoid using the "remember my password" feature associated with some websites, and disable this feature in your browser software. Always click on "Don't remember my password".

g) Do not store your password on any media unless it is protected from unauthorised access (e.g. encrypted with an approved encryption method).

h) When the user discover that his/her password has been used to access the system, the incident must be treated as a security violation and should be reported to Information Communication Technology immediately;

i) Change your password immediately if you believe that it has been compromised. Once done, notify the system/security administrator for follow up.

19.3 Password Administration

a) Old passwords must not be displayed at the time of typing the new password;

b) System Administrator must be able to revoke password;

c) Default passwords must have an enforced change on first use (temporary password has to be changed on the first log on);

d) User account shall be locked-out after three (3) invalid access attempts;

e) "*Annexure D*" shall be completed by the affected user and authorisation shall be granted by the Head of Department for the System Administrator to reset password or UserId;

f) Re-use of previous passwords must not be allowed.

20. Remote Access

20.1 Remote Access to Business Application systems is prohibited, unless authorised by the manager of the respective system;

20.2 A formal risk analysis process for applications to which remote access is granted to be performed to identify controls needed to reduce risks.

20.3 Remote user access shall be authorized by the Head of Department.

20.4 A register for all staff members authorized to use remote access facilities shall be maintained by the DISO.

20.5 A register of authorized remote access users and access levels provided shall be reviewed regularly by the System Administrator and DISO to confirm that there is still a valid business requirement.

20.6 Users are prohibited from altering or disabling any security features that have been enabled on wireless connections.

20.7 The following are approved network resources that will be allowed to be accessed utilising the internet:

(a) Remedy Online

(b) GroupWise

(c) Business related research

21. Internet and Email

21.1 Email shall be accessed by utilising login credentials.

21.2 Internet and Email access granted to Users shall not be abused and shall be utilised for work purposes only.

21.3 Uploading government information in free cloud services is prohibited.

21.4 Downloading of pirated and unlicensed software installation and files is prohibited and Users caught doing so shall be dealt with in accordance with disciplinary code of conduct.

21.5 Users shall sign Acceptable Usage of Internet and Email form.

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

22. All Business Application Systems (Transversal and Non-Transversal)

22.1 Only approved Users shall be provided with logical access to these systems.

22.2 Access to all Application Systems shall be monitored to ensure that passwords are changed regularly. See 19.1 (g).

22.3 Roles and responsibilities of system users shall be monitored by the System Administrator to ensure segregation of duties.

22.4 All systems breaches realised shall be reported to the Systems Administrator and Security and Facilities Management for investigation.

22.5 All systems policies and procedures shall be reviewed regularly by System Administrators, Users and/or ICT management.

22.6 All ICT systems shall be reviewed by System Administrator(s) and /or ICT management.

22.7 Request for access to any Departmental Application system within the control and accountability of Departmental ICT component shall be made through Annexure D: Logical Access Form.

23. Malicious Software

23.1 Malicious software, for the purpose of this document, refers to Virus, Trojans, Worms and Spyware.

23.2 It shall be ensured that Antivirus installed in systems is setup to scan desktops and mobile devices daily.

23.3 Knowledge base system will be utilised in order to keep record of types of Malwares the department has faced.

23.4 Users are prohibited from installing unauthorised software.

24. Firewalls and Antivirus

24.1 The Information Communication Technology shall ensure the activation of an effective desktop firewall and install anti-virus for the department.

24.2 It is the responsibility of Office of the Premier - IT to ensure the implementation of an effective network firewall and virus security strategy for the department.

24.3 It is the responsibility of the Information Communication Technology to ensure that the latest version of antivirus software is installed on all computers.

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

24.5 Users should not disable or interfere with the firewall status and the virus scanning software.

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

24.7 Upon the detection of a virus, Users should notify the ICT section for assistance immediately.

24.8 In cases of anti-virus license renewal delay by SITA and NWPG, the department shall install unlicensed / free software to ensure computers are protected from cyber attacks, viruses etc.

25. Incident Management

25.1 All the departmental ICT faults shall be reported to Office of the Premier - IT Helpdesk.

25.2 Remedy System will be the tool used for logging ICT incidents.

25.3 ICT incidents shall be prioritized according to the impact they have on the continuity of functions in the department and critical systems.

25.4 ICT Services and Standard manual was developed and implemented.

26. Classification

The Department shall ensure that information is classified according to the uniform sensitivity classification scheme below:

a) Public: this information has been approved by Accounting Officer for release to the public. Examples include reports, announcements, job

openings, press releases, service brochures, and information published on the departmental website.

b) Confidential: this information is private or otherwise sensitive in nature and must be restricted to those with a legitimate business need for access. The unauthorised disclosure of this information could adversely affect the department or third parties. Examples include employee performance evaluations, transaction data, agreements, unpublished memorandums and /or submissions, passwords, internal audit reports and all client information.

c) Secret: applies to the most sensitive business information which is intended strictly for use within a department and restricted to those with legitimate business need for access. The unauthorised disclosure of this information could seriously and adversely impact the department or third parties.

27. Information System Acquisition, Development and Maintenance

27.1 System development or changes to existing systems follow a formal structured approach whereby information security is considered at all stages of the system development life cycle.

27.2 Any System development, including development through a third party, follows an approved system development methodology outlined in the Service Level Agreements/contract and the methodology must include secure application design standards, secure coding practices, and security of third-party code.

27.3 All aspects of how information security is considered and implemented for all new systems or changes to existing systems shall be recorded.

27.4 The use of production data for development testing is prohibited unless such use is approved by the Accounting Officer.

27.5 Business Application systems can only go into production after users and information operations staff have received appropriate documentation and training on the relevant application security-related privacy.

27.6 The department shall ensure that ICT application is tested and scanned for vulnerabilities. Exploitable and other high-risk vulnerabilities shall be remedied before the application is used. Technical program documentation and end-user documentation shall be made available.

27.7 All Information system acquisition shall be procured in line with the Supply Chain Management procurement prescripts and SITA contracts.

27.8 Failure to procure information systems without following the Supply Chain Management procurement prescripts and SITA contracts shall constitute non-compliance.

27.9 The interest of the department in the ownership of the developed system and data should clearly be stated in the relevant contract.

27.10 Skills transfer of the development of the Information System shall also form part of the contract or Service Level Agreement.

27.11 All the developed applications should be audited to ensure that they fulfil the functions for which they were developed for.

28. Intellectual Property Rights

The department shall ensure that any system (software, information, source code, system design documents) developed by and/or on behalf of the department shall remain the intellectual property of the department and may therefore not be copied, sold, leased, or removed without the express of written consent of the relevant executive authority or delegated.

29. Physical Security Management

The Department shall ensure that:

a) Physical Security measures for all departmental ICT assets (i.e. lockable server rooms, switches, cabinets, and/or any other related physical assets that are restricted from public or unauthorised access) are put in place.

b) There is sufficient protection against environmental threats and hazards such as fire, theft, tampering, water damage and vandalism.

c) There is adequate security at the entrance of the data centre/ server rooms and other facilities where ICT Infrastructure is housed.

d) A generator and uninterrupted power supply is available to power critical ICT systems, and it is tested quarterly and maintained.

e) Confidentiality agreements and maintenance agreements are in place to ensure the security and confidentiality of the information stored on equipment that is subject to 3rd party and off-site access.

f) Users who are assigned devices, including portable computers of whatever nature, smartphones, tablets, and peripheral devices that contain government data or have been connected at any time to the government

network, do not leave these devices unattended in motor vehicles or public places.

g) All users (employees, contractors, and incidental users) are prohibited from making any hardware or software change to any shared server or network devices. If there is a business reason for making for making hardware or software change, a change request must be submitted following the departmental change management process.

h) Non-standard hardware configurations and security configurations (i.e. firewall settings, virtual and physical server setting, router, and switches) are considered for recommendation by the Provincial GITO.

i) Any loss or theft of information assets is treated as a security breach and reported immediately following the departmental loss procedure. Where necessary and applicable, a mobile device management tool must be implemented to assist with tracking and recovery of departmental laptops and notebooks.

j) Information assets containing departmental information must be securely stored or retained with the owner while traveling.

k) Process, procedures, or technical controls are in place to manage the risks associated with removable media (i.e. data leaks, data loss, data privacy, data sensitivity, malware infection, etc)

30. HR Security

30.1 HR Security Operations

The Department shall ensure that background verification checks or security vetting of contractors, and external party users are carried out under relevant laws, regulations, and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

30.2 User Responsibilities

The department shall ensure that:

a) All personnel are responsible for all activities performed with their user identities and special logon identities. As such, user identities and other logon identities may not be used by anyone other than the person to whom

they have been issued and users shall not perform any activity with identities belonging to other users.

b) Users submit a request to the Office of the Premier IT helpdesk to issue a new password if a password is forgotten, and users must prove their identity before the password is issued or reset.

c) Users report any misuse or unlawful use of user identities and passwords to the departmental ICT.

d) The unsuccessful login attempts are logged, and investigations should occur where unsuccessful login attempts are out of the normal range.

31. Communications and Operations Management

The department shall ensure that:

a) A formal change control procedure is documented and enforced to govern the application, computer installation, networks, and system development changes.

b) The system owner approves all business application changes with a financial impact.

c) ICT systems are accessed and authenticated through provincial network. The Provincial GITO shall approve secure emergency remote access/alternative network connection method.

d) Emergency changes that bypass some of the elements of established change control system, require the authorization of all affected business units and acknowledgement of the risks involved. These actions shall be controlled, logged, restored, and kept to a minimum.

e) Production systems are physically separated from test and development systems.

f) All activities related to changes of systems and performed using supervisory access rights will only be performed once appropriate authorization is received through the change control process, accompanied by change control documentation. This review shall be signed-off or electronically verified by the appropriate manager.

g) Approval and confirmation of the new ICT system satisfy all necessary security requirements before that system is used in a departmental environment.

32. Prohibited Software

a) All approved software shall be installed by ICT Technicians in the Departmental computing resources.

b) A list of approved software shall be developed and maintained to identify and prevent installation of malicious software.

c) Users are restricted to install software in computing resources. Only the IT Official with access to ICT Admin Account is allowed to install software in the Departmental computing resources.

33. ICT Disaster Recovery Plan

33.1 Information Backups

a) To a certain limit, Departmental information/data shall be regularly backed up on the Server.

b) Information Communication Technology shall facilitate the implementation of automated back up system with Office of the Premier - IT as back up mechanism for IT systems in the Department.

c) Only work-related information will be backed up on the server.

d) It is the responsibility of Users of Laptops to ensure that Laptops are connected to the network on regular basis in order to backup information/data.

e) Where need arises, the Supply Chain Management shall provide officials with removable devices for the storage of work-related information.

33.2 Backup of DCSTM servers

a) Backups of the systems database shall be done weekly on the Server via an automated process available in the operating system.

b) Regardless of classification, the availability of all data shall be maintained through periodic backups and recovery mechanisms.
c) Departmental backups shall be covered in the existing contract/ agreement of any service provider and backups containing sensitive data are encrypted.
d) The departmental minimum and maximum retention periods of information are based on contractual, legislative, regulatory, or industry requirements.
e) All archival backup data stored off-site shall be reflected in an up-to-date directory that shows the most recent date when the information was modified and the nature of the information.
f) All storage devices on which sensitive, valuable or critical information is stored for periods longer than six months shall not be subject to degradation. Such media shall be tested at least annually to ensure that the information is still recoverable.
g) Log files to be maintained on server confirming backup.
h) Bi-Monthly backups of the database and log files will be done.
i) Backups shall be done weekly and stored in a secure location by the System Administrator.
j) A register for the maintenance and management of backups to be maintained. Register will include the following:
    i. Identification of Backup (servername YYYY/MM/DD).
    ii. Name of official who made the backup, Signature and Date,
    iii. verification of backup (Name of Official, Signature and Date),
    iv. Random / Scheduled testing and restore of selected backup (Name of Official, Signature and Date, comment = successful or not),
    v. Provision for Monthly Sign off of Register By Programme Manager or delegated Official
    vi. Testing of backups will be done monthly by departmental system administrators.
    vii. Backup shall be stored in a secured offsite place by the System Administrator(s).

34. ICT Continuity Plan

34.1 ICT Continuity Plan shall be developed in line with the departmental Business Continuity Plan.

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

34.3 ICT Continuity plan shall be endorsed by the Departmental ICT committees.

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

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

35. Security Awareness Training

35.1 Information Communication Technology directorate in conjunction with Security and Facilities Management shall conduct Security awareness campaigns.

35.2 Both Information Communication Technology, and Security and Facilities Management shall develop and implement a continuous information security awareness program to reduce cybersecurity risks from employees in the department.

35.3 The awareness program shall make departmental users aware of internal security policies.

35.4 The information security awareness program shall train employees to recognise, and report cyberattacks (phishing, baiting, tailgating, etc) as well as train employees to properly handle (store, transfer, and destroy) sensitive data.

35.5 The information security awareness program must include security awareness or skills training targeted for specific roles including system administrators and application developers.

35.6 Security awareness could either be presented in a form of face-to-face engagement, posters, newsletters or utilising the intranet and emails.

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

35.8 An appropriate summary of the department's ICT Security Policy must be included in the HR contracts / policies that all employees sign before starting any work in a department. *(Annexure A)*

36. ICT Service Provider Management

a) The department shall ensure that there is a process to evaluate ICT service providers who have access to sensitive data or have a responsibility for ICT infrastructure to ensure the protection of data and infrastructure.

b) Security requirements must be included in the contracts of the service provider (Data encryption, multifactor authentication).

37. Use of ICT Information Assets

a) Access to administrator and root-level accounts shall be granted by GITO.

b) Supervisory access rights shall be allocated on a business need basis and will be limited to the minimum services and functions necessary. Additional security measures must be implemented to ensure that they are used only for the intended purpose.

c) The processes to control the allocation, revocation, and review of powerful rights are in place. These processes will include authorisation of all access rights by the appropriate line management and mechanism to ensure that access rights are adjusted appropriately should the person leave or change job description.

d) Critical logical access activities performed using powerful access rights generate audit trails and will be logged. All audit trails and logs shall be reviewed monthly by the system administrator and stored for one year.

e) Users shall not share usernames and shall be given unique usernames; therefore, no system generic usernames will be used.

38. Outsourcing Requirements

The Department shall ensure that:

a) Outsourcing complies with Condition 7 of Chapter 3 of the Protection of Personal Information Act, 2013 (Act No. 4 of 2013).

b) All consultants, temporary employees, and contractors must return all departmental property upon termination or expiration of their contract and all associated government network access (including remote access) rights should be simultaneously terminated.

c) External parties only use the information assets entrusted to them for the purposes agreed to in their contract.

d) The confidentiality and integrity of sensitive information will be protected when accessed through external party connections.

e) A formal risk analysis must be conducted for each external party connection and appropriate controls must be implemented to reduce risks to an acceptable level.

f) The external party users are restricted to the minimum services and functions necessary for the business process, as determined by the System owner.

g) As a condition of gaining access to a departmental computer network, every external party computer must be checked by DISO or delegated IT Official to ensure that the computer's antivirus software is up to date.

39. Cybersecurity

The department shall raise awareness on cybersecurity to ensure that departmental officials are aware of cyber threats and how to **prevent** them.

40. Cloud Security

The Department shall ensure that a thorough due diligence of the service provider's integrity, legal requirements, physical location, and security is conducted before deciding on a cloud service provider.

41. Electronic Signature

a) The Department shall ensure that the use of the electronic signature solution is approved by the Accounting Officer.

b) The Department shall ensure that the level of electronic signature selected is appropriate when considering the risks associated with a particular document or approval process.

42. Auditing and Monitoring

a) Office of the Premier IT shall ensure that audit log management (collect, alert, logs review and retain) occurs to detect malicious activities early. This includes the network traffic through both internal and external gateways, eg. Firewalls, email gateways, intrusion detections and routers monitored for unusual activity (for example, abnormal combinations of connections,

deliberate probing, or attacks, and unusually substantial amounts of data being transferred cross-border).

b) Systems to which external parties have access (such as client systems, web servers and dial-up support facilities) shall have all transactions and system configuration changes monitored in real-time, with alerts escalated to appropriate personnel where authorized transaction occur.

c) Computer clocks shall be synchronized to ensure accuracy of audit logs for investigations or as evidence in legal or disciplinary cases.

43. Compliance

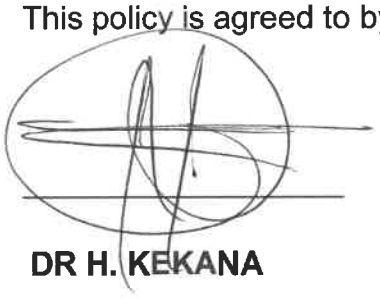
Any disciplinary action arising from non-compliance with this policy, procedures and guidelines shall be dealt with in accordance with Public Service Disciplinary Procedure.

44. Review

This policy shall be reviewed after a period of three (3) years or as and when there is a major change. This policy shall remain valid until the approval has been granted for the reviewed policy.

45. Approval

This policy is agreed to by the Accounting Officer.



04/12/2023

DR H. KEKANA **DATE**

ACCOUNTING OFFICER

Annexure A

Annexure A

ICT SECURITY POLICY DECLARATION FORM

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.

Security measures on integrity and confidentiality of personal information in terms of Chapter 3, Condition 7, 19 (1) of the Protection of personal information Act, 2013 states that, a responsible party must secure the integrity and confidentiality of personal information in its possession or under its control by taking appropriate, reasonable technical and organisational measures to present unlawful access to or processing of personal information. 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 on a quarterly basis, 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 cost 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

_____

Departmental staff member (as Witness)

dcstm
Department:
Community Safety and Transport Management
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

ICT ASSET MOVEMENT FORM

Tirelo Building, Albert Luthuli Drive,
Mafikeng, 2745
P/Bag X 19 Mmabatho 2735
Tel: +27 (18) 200 8020 / 8003

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.					

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

Department Stamp

ICT ASSET REALLOCATION FORM

ANNEXURE C

REASON FOR REALLOCATION:

Current user Information		New User Information	
Initials & Surname		Initials & Surname	
Office Number		Office Number	
Name of the building		Name of the building	
Head/Regional/ District Office		Head/Regional/ District Office	
ICT Technician		ICT Technician	
Contacts		Contacts	

No	Asset Bar Code #	Asset Serial #	Asset Description	Condition of Asset
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				

Movement of ICT Assets Sign Off			
Designation	Name	Signature	Date
Asset Holder (Old)			
Asset Receiver (New)			
IT Technician			

dcstm
Department:
Community Safety and Transport Management
North West Provincial Government
REPUBLIC OF SOUTH AFRICA

ICT LOGICAL ACCESS AUTHORIZATION FORM

ANNEXURE D

Applicant's Personal Details	
First Name	
Surname	
ID No.	
Email	
Phone Number	
Fax Number	
Company / Department	
Section	
Location	
User ID/Persal No	

Please Tick where applicable:

New User ID		Reset User ID		Reset Password		Request for Reports		Remove System Access	
Specify Application:			Specify Application:			Specify reports:		Specify Location:	

If not listed above, kindly describe your request in detail, e.g. Access to specific server and folder:

Please sign below:

Applicant:

Signature: _____ Date: _____

Duly Authorised by Sub Programme Manager/delegated:

Initials: ____ Surname: _____

Tel: _____

Signature: _____ Date: _____

Department Stamp