dcstm

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

2030 NDP

DEPARTMENT OF COMMUNITY SAFETY AND TRANSPORT MANAGEMENT

INFORMATION COMMUNICATION TECHNOLOGY END-USER POLICY

(ACCEPTABLE USE)

ICTEUP VERSION 1.0

Document Details

Author	Directorate Information Communication Technology
Department	Community Safety and Transport Management
Division Name	ICT Management
Document Name	Information Communication Technology End-User Policy
Sensitivity	Internal Use Only
Effective Date	<Date of Accounting Officer's signature>
Created Date	23-11-2023
Version Date	<Date of Accounting Officer's signature>
Version	ICTEUP-VERSION 1.0

Change Record

Modified Date	Author	Version	Description of Changes
	Directorate Information Communication Technology	1.0	Compliance to DPSA requirements

Stakeholder Sign–Off

Name	Position	Signature	Date
Mr O. Gabonnwe	Departmental Information Technology Officer		02/05/24
Ms K. Phatudi	Governance Champion		02/05/24
Ms F. Nchoe	Chairperson: ICT Steering Committee		02/05/24
Ms K. Phatudi	Chairperson: ICT Strategic Committee		02/05/24
Ms M.G. Mothibedi	Departmental Chief Risk Officer		02/05/24
Ms M. Mogatusi	Acting Director Legal Services		24/05/24

Records Management Sign–Off

Name	Position	Signature	Date
Mr E. Khuto	Deputy Director Records Management		24/05/2024

TABLE OF CONTENTS

GLOSSARY OF TERMS

Access control	A system to restrict the activities of users and processes based on the need-to-know
Contractors	A person or business which provides goods or services to the Department
Critical Information	Any information essential to departmental business activities, the destruction, modification, or unavailability of which would cause serious disruption to departmental business.
End-user	A user who employs computers to support business activities, who is acting as the source or destination of information flowing through a computer system.
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	means all aspects of technology that are used to manage an support the efficient gathering, processing, storing, and dissemination of information (Information Communication Technology).
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
NWPG	North West Provincial Government
User	Employee utilising ICT equipment
Virus	A parasitic software program, equipped with the means of reproducing itself, that spreads throughout a computer or network by attaching itself or infecting other software or diskettes. A worm is a similar program that propagates across a network by making

	copies of it.

1. LEGAL FRAMEWORK

- The Electronic Communications and Transactions Act (Act No. 25 of 2002)
- The Public Service Act (Act No. 111 of 1984)
- The Protection of Personal Information (Act No. 4 of 2013)
- The Protection of Information Act (Act No. 84 of 1982)
- The Minimum Information Security Standards (MISS)

This policy operates in conjunction with the following Departmental policies:

- The Approved ICT Security Policy
- The approved ICT User Account Management Policy

2. PURPOSE OF THE POLICY

The purpose of this policy is to ensure proper use of departmental ICT assets. This policy shall apply to any ICT assets that the department has or may install in the future, including but not limited to email, internet, mobile data cards, and desktop computing (including laptops and tablets). An acceptable use policy (AUP) is a document stipulating constraints and practices that a user must agree to for access to a provincial network, the internet, or other resources.

3. SCOPE OF APPLICATION

This policy is applicable to all users in the department, third parties, and contractors utilizing the departmental computing resources.

4. GUIDING PRINCIPLES

The purpose of the ICT end-user policy is to protect the Department of Community Safety and Transport Management, employees, contractors, third parties, and other stakeholders from illegal and damaging actions, whether intentional or unintended. The ICT assets allocated to departmental officials shall be utilized by employees for official purposes only as they are provided as working tools to enable employees to perform their official functions diligently.

5. USE OF ICT EQUIPMENTS

a) The end user shall be responsible for his/her workstation or portable device.

b) All losses or theft of computing resources must be treated as a security breach and to be reported to SAPS within 24 hours after acknowledgment of theft or loss.

c) All ICT equipment must be physically secured or protected to guard against theft;

d) Users must ensure that ICT equipment assigned to them has been added to the asset inventory and has received a unique asset number and classified in accordance with the Asset register.

6. DESKTOP COMPUTER USE

a) Users shall have a username and password to access the computer desktop or laptop.

b) Users must keep passwords secure and not share account credentials with anyone. Users are responsible for the security of their passwords and accounts.

c) The computing resources shall be locked or logged off when not attended.

d) ICT shall ensure that the computing resources are kept up to date with the latest anti-virus software and Operating System updates.

e) Users must not disable, and/or change the configuration of the anti-virus software.

f) 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.

g) Users shall not install any illegal software in computing resources e.g unlicensed anti-virus software, games.

h) Users acknowledge sole responsibility for any unauthorized or pirated software found in their possession or on the system and equipment allocated to them.

7. EMAILING SERVICES

Electronic mail usage is granted to support departmental business activities. The Department supports the installation and usage of the approved email by users. The IT Helpdesk shall assign the username and password to access emailing services.

7.1 Acceptable email use

- Electronic messages are frequently inadequate in conveying mood and context. Users should carefully consider how the recipient might interpret a message before composing or sending the message.
- In the absence of NWPG emailing services, authorization shall be granted by GITO and/or Accounting Officer to use private email to communicate government-related information. (*Use Annexure A*)
- Communication between officials and non-officials for business purposes.

7.2 Unacceptable email use

Unacceptable use hereto refers to usage of the departmental ICT resources i.e. Application of a computing system that is improper or undesirable e.g. carelessness, illegal activities and abuse.

The activities below are examples of unacceptable use; however, the list is not exhaustive.

- Creating and exchanging messages that can be interpreted as offensive, harassing, obscene, racist, sexist, ageist, pornographic or threatening.
- Opening file attachments from an untrustworthy source or with a suspicious or unexpected subject line.
- Sending confidential information to unauthorized people or violating the Minimum Information Security Standards.

- Promoting or publishing a User's political or religious views, operating a business or for any undertaking that offers personal gain.
- Using any e-mail system, other than the NWPG e-mail system, for departmental-related communications, unless authorised to use private email by the Accounting Officer and / or GITO.

8. INTERNET

Internet usage is granted for the sole purpose of supporting departmental activities necessary to carry out job functions.

8.1 Acceptable use of the internet

a) Accessing web-based applications and tools for official purposes.

b) Review of possible vendor websites for product information.

c) Reference regulatory or technical information in line with the relevant job description or official functions.

d) Accessing Government websites and portals.

e) Conducting research in line with your job function.

8.2 Unacceptable Uses of the Internet

The department prohibits engaging in fraudulent or corrupt activities or knowingly disseminating defamatory or pornographic material.

Activities that are strictly prohibited include, but are not limited to:

a) Accessing information that is not within the scope of the official's work.

b) Any conduct that would constitute or encourage a criminal offence, lead to civil liability or otherwise violates any regulations, directives, or the common law.

c) Using the internet for any purpose or in any manner that may prejudice the rights or interests of the Department of Community Safety and Transport Management or government in any other sphere.

9. ICT SECURITY

Departmental data is considered sensitive and confidential; therefore, all users or any other authorized user(s) must treat it as such. All users accessing departmental information shall preserve the confidentiality, integrity and availability of information. Users must handle all information resources in a secure manner.

10. COMPLIANCE

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

11. REVIEW

This policy will be reviewed every three (3) years or as and when the need arises. This policy shall remain valid until approval has been granted for the reviewed policy.

12. APPROVAL

This policy is approved by the Accounting Officer and is applicable with effect from the date of approval below.

DR H. KEKANA
ACCOUNTING OFFICER

06/05/2024
DATE

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

INFORMATION COMMUNICATION TECHNOLOGY

Tirelo Building, Albert Luthuli Drive,
Mafikeng, 2745
P/Bag X 19 Mmabatho 2735
Tel: +27 (18) 200 8010/ 8163

ICT REQUEST TO USE PRIVATE EMAIL AUTHORIZATION FORM

ANNEXURE A

Applicant's Details	
First Name	
Surname	
ID No.	
Email	
Phone Number	
Section/ Directorate	
Location	
Persal No	

I am entrusted with the responsibility of ________________________________. I hereby request authorization to use private email to send and receive official emails for the financial year ___________. As a member of the Department of Community Safety and Transport Management, I believe that access to this resource (emailing services) will greatly benefit my work and enable me to complete my tasks more efficiently during the interruption and/or unavailability of access to the North West Provincial Government emailing services.

I understand that access to this resource may require additional security measures, and I am willing to comply with any requirements necessary to gain access.

Please sign below:

Applicant:

Signature: ______________________ Date: ________________

Duly Authorised by Accounting Officer/delegated:

Initials: ____ Surname: ____________________

Tel: _____________________

Signature: __________________ Date:__________________

Department Stamp

"Let's Grow North West Together"

DECADE OF ACTION FOR ROAD SAFETY 2021 - 2030

ARRIVE ALIVE