Department of Public, Works Roads and Transport

Mpumalanga Provincial Government

ICT END USER POLICY (ACCEPTANCE USE)

Issue	01
Responsible Section	Knowledge Management
Date of approval	13/07/2026

MPUMALANGA
THE PLACE OF THE RISING SUN

TABLE OF CONTENTS

ABBREVIATIONS

AO	: Accounting Officer
AUP	: Acceptable Use Policy
CGICTPF	: Corporate Governance of ICT Policy Framework
DPWRT	: Department of Public Works, Roads and Transport
E-MAIL	: Electronic Mail
GCCN	: Government Common Core Network
ICTOC	: Information Communication Technology Operational Committee
ICTSC	: Information Communication Technology Steering Committee
IT	: Information Technology
LAN	: Local Area Network
MPG	: Mpumalanga Provincial Government
MPSA	: Minister of Public Service and Administration
PC	: Personal Computer
PIN	: Personal Identification Number
WAN	: Wide Area Network
WWW	: World Wide Web

1. INTRODUCTION

1.1. The current digital era has seen the increased importance of data and information, thus giving it the status of being the economy's raw material. It has brought the importance of protecting data and information to ensure its confidentiality, integrity, and availability.

1.2. In line with this, section 3(1)(f) of the Public Service Act, as amended, the Minister of Public Service and Administration (MPSA) must establish norms and standards relating to information management to improve the efficiency of the public service in terms of internal operations and service delivery.

1.3. Against this background, the Department of Public Works, Roads and Transport developed the end user policy (acceptable use) IT Security policy that will give guidance in establishing information security governance, practices, and procedures to protect its information technology assets.

2. PURPOSE

The objectives of this policy aim to promote proper and acceptable usage of IT solutions / resources.

3. REGULATORY FRAMEWORK

3.1 Communication Security Act 2002 (Act No. 68 of 2002)

3.2 Copyright Act, 1978 (Act No. 98 of 1978)

3.3 Corporate Governance of ICT Policy Framework (CGICTPF)

3.4 Electronic Communication and Transaction Act, 2000 (Act No. 25 of 2002)

3.5 Information Act, 2000 (Act No. 70 of 2002)

3.6 Integrated ICT Policy (IICTP)

3.7 Minimum Information Security Standards (MISS)

3.8 National Cyber Security Policy Framework

3.9 Networking Standards (ISO)

3.10 Occupational Health and Safety Act, 1993 (Act No. 85 of 1993)

3.11 Promotion of Access Information Act, 2000 (Act No. 2 of 2000)

3.12 Protection of Personal Information Act, 2013 (Act No.4 of 2013)

3.13 Public Finance Management Act, 1999 (Act No.1 of 1999)

3.14 Public Service Act, 1994 (Act No. 103 of 1994)
3.15 State Information Technology Agency (SITA) Act. 1998 (Act No. 88 of 1998)

4. SCOPE OF APPLICATION

This policy shall be applicable to:

4.1 All officials of DPWRT.

4.2 Consultants, contractors, learners / interns or any third party authorized to use DPWRT facilities.

4.3 All IT solutions, that is, computer resources, systems and networks that are owned or leased by the Department.

5. POLICY STATEMENTS

The Departmental ICT assets are provided to support service delivery, communication, and administrative functions. All officials are required to utilize the Departmental ICT assets responsibly, ethically, securely, and in accordance with applicable regulations, legislation, policies, and procedures.

All officials shall ensure that Departmental ICT assets, including but not limited to computers, mobile devices, email system, internet services, software, networks, and electronic information are used primarily for authorized purposes and in a manner that protects the confidentiality, integrity, and availability of the Departmental information and systems.

All officials shall adhere to the following:

5.1 Acceptable Use

5.1.1 Connecting to DPWRT IT resources is a "privilege" and not a right.

5.1.2 "Strong passwords" (a combination of letters, numbers, symbols and characters e.g. @-*# $%! 1-9 Aa? {} A&) shall be used when logging in to computer resources.

5.1.3 Passwords should be treated as confidential.

5.1.4 Passwords should be changed regularly.

5.1.5 A "compromised password" shall be changed immediately.

5.1.6 Every computer machine should have an auto-lock login screen saver.

5.1.7 Always lock your computer when you temporarily leave your desk (Press Windows Flag button +L).

5.1.8 Every individual user should ensure that documents are backed up in the available backup system.

5.1.9 Every official assigned with IT resources is responsible and accountable for its security.

5.2 Prohibited Use

5.2.1 Illegal or Unauthorized Access (hacking) to other people's computers or accounts is prohibited.

5.2.2 Weak passwords or easy to guess passwords.

5.2.3 The installation of illegal or unauthorized software.

5.2.4 The sharing of passwords and user accounts.

5.2.5 The use of DPWRT systems and networks for fraudulent activities.

5.2.6 The tempering with computer machines (striping and or opening).

5.2.7 Unauthorised disclosure of DPWRT information.

5.2.8 The playing of illegal multi-media applications; (define multimedia).

5.2.9 Unauthorised viewing or browsing of files or accounts of other people.

5.2.10 Spamming (mass e-mails)- to be avoided or done with management permission.

5.2.11 Misuse of the E-mail system and internet the distribution of disruptive messages on sex, disability, religion, race etc.

5.2.12 The sending of unsolicited and or offensive e-mail messages to other people.

5.3 Enforcement

5.3.1 Violations of this policy may result in disciplinary action in line with Departmental policies, up to and including termination of employment, recovery of damages, and legal action where applicable.

5.3.2 Relationships with all external stakeholders, including contractors and third parties, will be governed by this policy and the contracts signed between the Department and Stakeholders.

6. ROLES AND RESPONSIBILITIES

6.1 **Accounting Officer:** Responsible for the effective and efficient implementation of this policy as part of internal controls within the Department.

6.2 **ICT Governance Committee:** Oversight of ICT usage, compliance monitoring, and policy review.

6.3 **ICT Unit:** Implementation of security controls, monitoring systems, and user support.

6.4 **Employees/Users:** Responsible for adhering to this policy and safeguarding IT resources.

7. MONITORING AND EVALUATION

Management Information System section shall monitor and evaluate the implementation of this policy.

8. POLICY REVIEW

The policy shall be reviewed every 5 years or as and when there is a need to factor changes in legal frameworks as well as economic trends.

9. DEVIATIONS

Any deviation from this policy shall be subject to the approval of the Accounting Officer.

10. IMPLEMENTATION DATE

This policy shall come into effect from the date of approval by the Accounting Officer.

11. APPROVAL

MR RIKHOTSO
A) HEAD: PUBLIC WORKS, ROADS AND TRANSPORT
DATE 13/07/2026