



Department of Public Works, Roads and Transport

MPUMALANGA PROVINCIAL GOVERNMENT

INFORMATION TECHNOLOGY (IT) SECURITY POLICY

Issue:04

Responsible Section: Knowledge Management

Date of Approval:

TABLE OF CONTENTS

Item/ Topic	Page
Abbreviations	2 - 3
Definitions	4 - 5
Introduction	6 - 8
Objectives	8
Regulatory Framework	8 - 9
Scope of Application	9
Policy Statement	9 - 21
Roles and Responsibilities	21
Monitoring and Evaluation	21
Policy Review	21
Deviations	21
Implementation Date	22
Approval	22
Annexure 1: PROCEDURES 1A: BACKUP AND RESTORE 1B: DISPOSAL OF IT SOLUTIONS 1C: ACCESS CONTROL	23 -26
Annexure 2 : SOCIAL MEDIA GUIDELONES	27

10/18

ABBREVIATIONS

AO	: Accounting Officer
AUP	: Acceptable Use Policy
CGICTPF	: Corporate Governance of ICT Policy Framework
DPWRT	: Department of Public Works, Roads and Transport
DRP	: Disaster Recovery Plan
E-MAIL	: Electronic Mail
ETC	: et cetera
FTP	: File Transfer Protocol
GCCN	: Government Common Core Network
ICTOC	: Information Communication Technology Operational Committee
ICTSC	: Information Communication Technology Steering Committee
IICTP	: Integrated ICT Policy
I&RM	: Information and Records Manager
IS	: Information Systems
ISO	: International Standards Organization
ISS	: Information and Security Systems
IT	: Information Technology
ITB	: Information Technology Bureau
LAN	: Local Area Network
MISS	: Minimum Information Security Standards
MPG	: Mpumalanga Provincial Government
NDA	: Non-Disclosure Agreement
PC	: Personal Computer
PIN	: Personal Identification Number
SACSA	: South African Communication Security Agency
SITA	: State Information Technology Agency

SLA : service Level Agreement
SRC : Security and Risk Management Committee
VS : Vice versa
WAN : Wide Area Network
WWW : World Wide Web

1/21

DEFINITIONS

Accounting Officer	means	a person appointed as defined in the Public Finance Management Act, 1999 (Act No.1 of 1999);
Consultant	means	a person or company engaged by the Department to do business on their behalf;
Cryptography	means	the science of transforming information into unreadable format (or the encryption of data);
Illegal	means	lacking permission and not authorized;
Information Systems	means	applications and systems used to process data utilizing Information Technology (IT) as an enabling tool;
Information Technology	means	the processing of data via a computer/s. These are aspects of technology that are used to manage and support the efficient gathering, processing, storing and dissemination of information as a resource. Information Technology is a data processing enabler;
IT Incident	means	means an adverse in an information system and/or network or the threat of the occurrence of such an event.
IT Solutions	means	all IT Hardware and Software resources e.g. Personal computers, laptops, printers, Systems and all other IT-related Services;
Local Area Network	means	a group of computers connected as on a network. A communication infrastructure that enables users to share resources such as printers, software, data, etc. in a way that is cost-effective;
Monitoring	means	the actions directed at measuring performance to ensure the confidentiality, availability and integrity of systems and information;

Password	means	security code or pin code;
Server	means	file server or Document server;
SITA	means	State Information Technology Agency (SITA) established in 1999 through a special act of parliament to consolidate and coordinate the State's Information Technology resources;
System Owner	means	means a person or organization having responsibility for the development, procurement, integration, modification, operation, maintenance, and/or final disposition of an information system.
User	means	a person using computer equipment and network resources of the Department of Public Works, Roads & Transport (DPWRT);

10

1. INTRODUCTION

The purpose of this policy is to enable the Department of Public works, Roads and Transport (DPWRT) to apply an effective and consistent level of security to all its information and information systems.

Every organization depends on information as a vital asset to make informed decisions.

The Department critically depends on information and information systems and seeks to protect its information and information systems from loss, misuse and damage.

Through this policy, the Department seeks to ensure that the **confidentiality**, **integrity** and **availability** of its information are maintained by implementing best practices to minimize any potential risk to information.

Failure to comply with this policy shall be considered as misconduct and depending on the circumstances and seriousness of the offence, appropriate disciplinary action shall take place.

The policy therefore sets the tone and presents the philosophy of information security within the Department and also based on the following profound security principles:

The principles of the policy provide the ethical and moral essence and fundamental basis on which the Department's good business practice, policies and planned action are based.

1.1 PRINCIPLES

- 1.1. **Proportional Cost vs. benefit:** All security measures shall be appropriate and proportional to the cost and benefit of implementing such measures for which they are designed to protect;
- 1.2. **Adversary:** All security measures shall be established in the anticipation of natural disaster, harmful intent and hostile attack;
- 1.3. **Least Privilege:** Access to any IT system shall be granted on the basis of business need to access the facility in other words, the need-to-know basis;
- 1.4. **Separation of Duty:** Job functions shall be divided amongst co-workers. For example, no one person shall have access to both add employees to the Human Resources System and authorise payment for these people. No one

person shall have access to place an order and pay a supplier;

- 1.5. **Ethics:** In the implementation of the policy, the Department adheres to an ethical code of conduct in relation to monitoring and accessing of user accounts. An ethical judgement in this regard may need to be made;
- 1.6. **Timelines:** Employees and Third Party/s shall act or respond within a reasonable time period to any identified risk or security breach;
- 1.7. **Confidentiality:** Unauthorised disclosure of information is prohibited;
- 1.8. **Integrity:** Unauthorised modification of information is prohibited;
- 1.9. **Availability:** Refers to both Data and Service. Data shall be accessible when required;
- 1.10. **Controlled Access:** Information assets shall only be used for business purposes and for the business purpose intended;
- 1.11. **Levels of Protection / Assurance of protection / multiplicity of protection:**
In accordance with MISS, the following levels of classification shall determine the levels of protection –
 - 1.11.1. Restricted;
 - 1.11.2. Confidential;
 - 1.11.3. Secret; and
 - 1.11.4. Top Secret.
- 1.12. **Protected measure baseline:** The Department information is an important asset that shall be protected according to its value and degree of damage that could result from its misuse, unavailability, destruction, unauthorised disclosure or modification. This implies that information assets shall be identified, valued, assessed for risk and protected cost effectively from identified threats in accordance with the principle of Cost vs Benefit;
- 1.13. **Continuity of Protection:** The Department's information is an important asset that shall be protected at all times;
- 1.14. **System Stability:** The Department information is an important asset that shall be available as and when required. This shall entail all times unless otherwise specified;
- 1.15. **Survivability:** The Department information is an important asset that shall

have the ability to be sustained in the event of a disaster. Disaster Recovery Plans (DRP) shall be established and structured walk-through testing shall be done. Implementation of the plans shall be managed on a project-to-project basis; and

- 1.16. **Individual Accountability:** Every individual is accountable for the security of the Departmental assets under their control. The delegation of responsibility for security is assigned to each and every user within the Department. Mechanisms such as User Id's are in place to ensure individual accountability.

2. OBJECTIVES

The purpose of this policy is to:

- 2.1. Promote information protection and Systems security;
- 2.2. Protect information and information systems from loss, misuse and damage;
- 2.3. Promote proper usage of IT solutions; and
- 2.4. Provide guidelines on the acquisition of IT solutions

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);
- 3.16. Constitution of the Republic Of South Africa, 1996.

4. SCOPE OF APPLICATION

This policy shall be applicable to:

- 4.1. All officials of DPWRT including district offices;
- 4.2. Consultants, contractors, learners / interns or any third party authorized to use DPWRT facilities; and
- 4.3. All IT solutions, that is, computer resources, systems and networks that are owned or leased by the Department.

5. POLICY STATEMENTS

5.1 SECURITY

5.1.1 SECURITY MANAGEMENT

5.1.1.1. Information security shall be coordinated and supported at Senior Management level in the Department. It is the responsibility of Senior Management to support and ensure that the necessary Information and Security Systems (ISS) endeavours and initiatives are coordinated and enjoys the necessary privileges;

5.1.1.2. The Security Committee and Risk Management Committee responsible for all IT security related issues must be put in place. This must be composed of representatives from the following sections, IT, Risk Management, Internal Audit and Security management. Representatives from other Business Units can be co-opted as and when required; and the following security management aspects must be addressed by the Security Committee

- a) Information Security Awareness;

MT

- b) Manage the Department Security Program;
- c) Business Continuity and Disaster Recovery ;
- d) IS Risk Management; and
- e) IS Audit and Review.

5.1.2 PERSONNEL SECURITY

- 5.1.2.1. The employees of the Department accessing information systems and the data processed by the systems shall meet the necessary security requirements as determined by the sensitivity of information accessed;
- 5.1.2.2. Access to the systems and data shall be immediately terminated as soon as evidence of non-compliance with the security requirements is picked-up;
- 5.1.2.3. Information security roles and responsibilities shall be included in approved Job descriptions where required;
- 5.1.2.4. All employees who use IT services are required to acknowledge acceptance of and intention to comply with the Acceptable Use Policy by signing the Department Information Technology User Declaration Agreement. Any employee found to have violated this policy shall be subjected to appropriate disciplinary action;
- 5.1.2.5. All Third Party organisations are required to sign a Non-Disclosure Agreement (NDA) before access to any IT resource/s is/are permitted;
- 5.1.2.6. All access to DPWRT network shall require a unique username and password and
- 5.1.2.7. The proper use of passwords to manage access to systems is critical.

5.1.3 NETWORK SECURITY

- 5.1.3.1. The State Information Technology Agency (SITA) Government Common Core Network (GCCN) Security Policy shall apply for the Wide Area network (WAN) connections to DPWRT's network sites to

124

ensure the safeguarding of information on networks and the protection of the supporting infrastructure;

5.1.3.2. Defaults accounts (guest, supervisor or administrator) shall be configured to meet the Departmental requirements;

5.1.3.3. All connections to the DPWRT's Local Area Network (LAN) shall be authorized by the Accounting Officer;

5.1.3.4. Secure remote access shall be strictly controlled. Control shall be enforced via one-time password authentication or public / private keys with strong pass-phrases; and

5.1.3.5. Administrator passwords shall be kept sealed in a fireproof safe and known to at least two (2) persons.

5.1.4 UNLICENSED AND UNAUTHORIZED SOFTWARE

5.1.4.1. Under no circumstances shall illegal software be loaded on official computer;

5.1.4.2. The IT Section has the right to remove any such illegal software without prior notification; and

5.1.4.3. All officials are not allowed to install unauthorized soft wares without prior approval from the Accounting Officer.

5.1.5 PHYSICAL SECURITY

5.1.5.1. The Minimum Information Security Standard (MISS) applies. The Security Management policy of the Department shall be consulted for issues on physical security. All security areas / buildings where computer related equipment is used shall be classified according to its criticality in terms of risk and be protected to conform to the applicable standard of security;

5.1.5.2. Where feasible access to the Server rooms shall be strictly controlled and restricted to authorized personnel. Authentication controls like swipe cards or Personal Identification Number (PIN) shall be used to authenticate and validate access. An Audit trail shall be securely maintained;

18

- 5.1.5.3. Where feasible Fire prevention standards and procedures shall be established and adhered to in order to prevent fire from starting spontaneously due to negligence or as a result of arson. Firefighting equipment, sensitive to electronic environments and thermal shock on magnetic media, shall be deployed in high-risk areas. Fire detecting sensors (heat and smoke) shall be linked to an alarm system and shall be regularly tested;
- 5.1.5.4. Firefighting and evacuation procedures shall be adhered to and personnel shall be trained in the effective execution of these procedures. (Reference: Security Policy);
- 5.1.5.5. An access control system and procedures shall be implemented to control the movement of personnel and visitors on these areas; and
- 5.1.5.6. A removal control system and procedures shall be implemented for all computer related equipment entering or leaving Departmental offices.

5.1.6 SERVER SECURITY

- 5.1.6.1. All servers hosting data and applications shall be located in a physically secured environment where access is strictly controlled;
- 5.1.6.2. All server rooms and/or patch rooms shall be regarded as high-risk security areas and access to these areas shall be strictly controlled;
- 5.1.6.3. All servers shall be loaded and protected with the latest approved anti-virus software. Updates for patches and upgrades shall be implemented regularly;
- 5.1.6.4. Only an authorized administrator shall be granted administrative rights on the servers. Administrative password shall be kept secret and only nominated personnel at management's discretion shall have access to the password; and
- 5.1.6.5. Servers shall be backed up in accordance with the DPWRT backup procedures.

5.1.7 WORKSTATION SECURITY



- 5.1.7.1. All workstations shall be located in a physically protected environment where access control measures are in place and applied consistently. It shall be ensured that unattended equipment has appropriate security protection;
- 5.1.7.2. All workstations shall be loaded and protected by the latest approved Anti-Virus software;
- 5.1.7.3. It is the responsibility of the workstation user to ensure that appropriate security measures and practices are adhered to;
- 5.1.7.4. Users shall not leave their workstations unattended while accessing or processing information without appropriate protection like password protected screen savers;
- 5.1.7.5. Workstations used to access classified, secret or top secret, information shall at least be protected by two-factor authentication. For example encryption, smart cards, tokens
- 5.1.7.6. Users shall not share workstation passwords and user accounts with anyone;
- 5.1.7.7. It is the responsibility of the workstation user to ensure that his/her workstation is adequately protected from logical threats as well as physical environmental threats; and
- 5.1.7.8. All workstations must be connected to the network to ensure proper back up and anti-virus updates.

5.1.8 PASSWORD SECURITY

5.1.8.1 STRONG PASSWORDS.

All user-chosen passwords for computers and networks shall be difficult to guess. Personal details such as spouse's name, car number plate, Identity number, and birthday shall not be used unless accompanied by additional unrelated characters.

5.1.8.2 DISPLAY AND PRINTING OF PASSWORDS.

Handwritten mark

The display and printing of passwords shall be masked, suppressed, or otherwise obscured so that unauthorized parties shall not be able to observe or subsequently recover them.

5.1.8.3 PERIODIC PASSWORD CHANGES.

All users shall be required to regularly change their passwords.

5.1.8.3 CHANGING OF GIVEN PASSWORDS.

The initial passwords issued by a security administrator shall be valid only for the involved user's first on-line session. At that time, the user shall be forced to choose another password before any other work can be done.

5.1.8.4 ACCOUNT LOCKOUT.

A user's account will be locked after three unsuccessful logon attempts and only the system administrator can unlock user accounts.

5.1.8.5 IDENTIFICATION.

Users shall have a unique user name and passwords to identify them on the systems.

5.1.8.6 ACCEPTABLE USE POLICY (AUP)

This AUP clause constitutes the code of conduct for all users of our IT resources.

5.1.8 ACCEPTABLE USE

5.1.8.1. Connecting to DPWRT IT resources is a **“privilege”** and not a right;

5.1.8.2. **“Strong passwords”** (a combination of letters, numbers, symbols and characters e.g. @-*_#_! 1-9 Aa?{}^&) shall be used when logging in to computer resources;

5.1.8.3. Passwords should be treated as confidential;

5.1.8.4. Passwords should be changed regularly;

- 5.1.8.5. A “**compromised password**” shall be changed immediately;
- 5.1.8.6. Every computer machine should have an auto-lock login screen saver;
- 5.1.8.7. Always lock your computer when you temporarily leave your desk (Press **Windows Flag button +L**);
- 5.1.8.8. Every individual user **should ensure** that documents are backed-up (see Annexure. A); and
- 5.1.8.9. Every official assigned with IT resources is responsible and accountable for its security.

5.1.9. PROHIBITED USE

- 5.1.9.1. Illegal or Unauthorized Access (hacking) to other people’s computers or accounts is prohibited;
- 5.1.9.2. **Weak passwords** or easy to guess passwords;
- 5.1.9.3. The installation of **illegal or unauthorized software**;
- 5.1.9.4. The **sharing of passwords and user accounts**;
- 5.1.9.5. The use of DPWRT systems and networks for fraudulent activities;
- 5.1.9.6. The **tempering** with computer machines (stripping and or opening);
- 5.1.9.7. Unauthorised disclosure of DPWRT information;
- 5.1.9.8. The playing of illegal multi-media applications; (define multimedia or attach.
- 5.1.9.9. Unauthorised viewing or browsing of files or accounts of other people;
- 5.1.9.10. **Spamming (mass e-mails)** – to be avoided or done with management permission;
- 5.1.9.11. Misuse of the E-mail system for the distribution of disruptive messages on sex, disability, religion, race etc.; and
- 5.1.9.12. The sending of unsolicited and or offensive e-mail messages to other people.

5.1.10. ENCRYPTION

5.1.10.1. All communication over Mpumalanga Provincial Government (MPG) WAN and / or MPG LAN to LAN communication over the WAN classified confidential, secret or top secret shall be encrypted with approved South African Communication Security Agency (SACSA) cryptographic devices before transmission; and

5.1.10.2. Where encryption is not used for the transmission of classified information, it shall be reported as a breach of security to the IT section.

5.1.11 SECURITY AND PROTECTION OF RECORDS

For details of the security and protection of records refer to the approved Information & Records Management policy.

5.1.12 THIRD PARTY CONNECTIONS SECURITY

5.1.12.1. Third Party Persons shall have approval of the Accounting Officer to access DPWRT Network;

5.1.12.2. All approved changes shall be monitored to ensure that they are implemented according to specification;

5.1.12.3. The effects of changes shall be analysed before changes are approved and implemented; and

5.1.12.4. It is the responsibility of management to ensure that all approved changes to critical IT resources are at a minimal level of risk to the IT infrastructure.

5.1.13 FIREWALL

5.1.13.1. Information Technology Management shall tightly control the physical access to the firewalls, allowing only the firewall administrators and network services manager physical access to the servers;

- 5.1.13.2. The Firewall Administrator is responsible for Firewall configuration tables to determine what is permitted in or denied;
- 5.1.13.3. Rules shall be established as to which incoming and outgoing services shall be denied or allowed for various client/servers (e-mail, ftp, telnet, www, etc.);
- 5.1.13.4. Standards shall be established to stipulate which service utilizes specific port numbers. All services and connections through the firewall shall be denied unless specifically permitted by the Network Administrator;
- 5.1.13.5. The firewall shall log all reports on daily, weekly, and monthly bases to allow the analysis of the network activity through the firewall;
- 5.1.13.6. Firewall administrators shall audit the firewall logs in a timely manner (daily, if possible) to detect possible attacks from the Internet; and
- 5.1.13.7. Threat and vulnerability analysis shall be performed continuously (3 months).

5.2 INFORMATION TECHNOLOGY

5.2.1 PROCUREMENT OF IT SOLUTIONS

All applications to acquire IT solutions shall be in line with the procurement policy of the Department.

5.2.2 MANAGEMENT AND USAGE OF IT SOLUTIONS

5.2.2.1. It is the sole responsibility of IT officials to configure, install and repair IT solutions. No any other official is allowed to temper with IT solutions; and

5.2.2.2. The IT section's responsibility is to ensure that all IT solutions are functional and used properly by the Department.

5.2.3 THE USER'S RESPONSIBILITIES INCLUDE:

5.2.3.1 To ensure that IT solutions allocated to individuals are secured against loss by theft, fraud, malicious or accidental damage and any other illegal activity; and

5.2.3.2 To report to IT section any faults or malfunctioning or any suspicious activity occurring on the IT solution.

5.2.4 MANAGEMENT OF IT INCIDENTS

5.2.4.1. An Incident Management team shall be formed to execute the following tasks:

- a) Receive notification of incidents;
- b) Investigate incidents;
- c) Draft a report providing detail of the incident and accompanying evidence;
- d) Report the findings to the AO immediately;
- e) Escalate all incidents affecting information systems to IT
- f) Escalate all incidents affecting physical security to the Security Manager;

5.2.4.2 An Incident include the following:

- a) Network attacks;
- b) Denial of services;
- c) Theft;
- d) Infrastructure compromise;
- e) Virus infections;
- f) Availability and integrity compromise;
- g) Fraud;
- h) Illegal activity; and
- i) Incident that requires investigation of electronic documents.

5.2.5 PRIVATE EQUIPMENT

Private equipment must only be allowed for DPWRT's legitimate business need after approval from the Accounting Officer.

5.2.6 ELECTRONIC MAIL

- 5.2.6.1 As a productivity enhancement tool, the Department encourages the business use of electronic communications. Electronic communications systems, and all messages that are generated on or handled by electronic communications systems, including backup copies, are considered to be the property of MPG;
- 5.2.6.2 MPG electronic communications systems generally shall be used only for business purpose. Employees are reminded that the use of corporate resources, including electronic communications, should never create either the appearance or the reality of inappropriate use;
- 5.2.6.3 Misrepresenting, obscuring, suppressing or replacing the identity of a user on an electronic communications system is forbidden. The user name, electronic mail address, organizational affiliation and related information that are included with electronic messages or postings shall reflect the actual originator of the messages or postings;
- 5.2.6.4 The Department management shall regularly monitor the content of electronic communications. Content and usage of electronic communications shall be monitored to support operational, maintenance, auditing, security and investigative activities;
- 5.2.6.5 Recognizing that some information is intended for specific individuals and shall not be appropriate for general distribution, electronic communications users shall exercise caution when forwarding messages. The Department sensitive information shall not be forwarded to any party outside DPWRT without the prior approval of IT & Information and Records Management (I&RM) Manager; and
- 5.2.6.6 Users shall be aware of the classification of any information contained in data files or correspondence which they are

transporting using email communication and do not exchange information in un-encrypted form which is confidential.

5.2.7 INTERNET POLICY

- 5.2.7.1 Access to the Internet shall be granted to employees that have a legitimate need for such access, the user needs to formally apply for access;
- 5.2.7.2 All Internet connections shall be via the approved Internet service provider of the Department. Any other connections are prohibited;
- 5.2.7.3 Use of Internet is a privilege, which constitutes the acceptance of responsibilities, and obligations that are subject to government policies and laws. Acceptable use shall be legal, ethical, and respectful of intellectual property, ownership of data, systems security mechanism and individual rights to privacy from intimidation, harassment and annoyance;
- 5.2.7.4 All users shall authenticate themselves at MPG internal Web proxy server before gaining access to the Internet. This authentication process shall be achieved by logging on to the Internet via user name and password system;
- 5.2.7.5 To protect MPG from profane material and to minimize the use of bandwidth, all Internet usage shall be monitored by Web content filtering software;
- 5.2.7.6 Misrepresenting, obscuring, suppressing or replacing the identity of a user on the Internet or any MPG communication systems is forbidden;
- 5.2.7.7 Users shall not publicly disclose internal DPWRT information via the Internet, which could adversely affect DPWRT, customer relations or public image;
- 5.2.7.8 Users shall be subject to limitations on their use of the Internet as determined by the appropriate supervising authority;
- 5.2.7.9 MPG content filtering software shall prevent users from connecting to certain non-business web sites. All web sites that

contain sexually explicit, profane and other potentially offensive material shall be blocked out via the proxy server; and

5.2.7.10 At any time and without prior notice, the Department management reserves the right to examine Web browser cache files, Web browser bookmarks and other information that is stored on or passing through the computers of the Department. Such management access assures compliance with internal policies, assists with internal investigations and assists with the management of the Department.

5.2.8 SOCIAL MEDIA GUIDELINES

Refer to Government Communication policy as approved by Cabinet in August 2018;

6. ROLES AND RESPONSIBILITIES

6.1 The Accounting Officer shall be accountable for this policy and shall ensure adherence thereto; and

6.2 All officials and stakeholders in the Department shall be aware of this policy and properly execute their duties in line with the implementation of this policy.

7. MONITORING AND EVALUATION

The ICT Management shall monitor and evaluate the implementation of this policy.

8. POLICY REVIEW

The policy shall be reviewed to factor changes in legal frameworks, organizational developments, political and economic trends, and envisaged outputs of the Medium Term Expenditure Framework as well as outcomes of monitoring and evaluation.

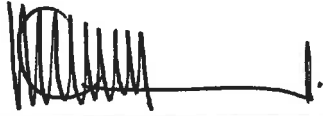
9. DEVIATIONS

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 MC MOROLO
HEAD: PUBLIC WORKS, ROADS AND TRANSPORT
DATE 13/12/2022.

Annexure 1: PROCEDURES

1. A BACKUP AND RESTORE

Purpose

This procedure is aimed at achieving the following objectives:

- a) Regular backups of files and pertaining backup be conducted,
- b) Regular testing of these backup files to ensure the integrity thereof,
- c) Regular testing of disaster recover (DRP) scenarios,
- d) Monitoring of outputs to ensure the processes are being actuated to facilitate continuity;
- e) Enhance good corporate governance and IT governance practices.

The purpose of this procedure is to provide a clear process regarding the backup and restore regime of end point files.

Scope

This procedure applies to all IT solutions used in the Department e.g. hardware and software. Leased and privately owned IT solutions used to perform official duties shall be affected by this procedure.

Process;

Automated backup – Automated backup subscribing to a daily, weekly and monthly schedule must be provisioned.

Offsite backup – The backup data must be distributed to servers at SITA switching centre.

Backup file integrity check – A supporting (Parallel) process needs to be provisioned whereby the integrity of the backup files is automatically verified.

Process monitoring – Outputs from the backup and integrity verification must be saved and emailed to the IT Manager. The IT manager must review the outputs weekly and file them (deemed signed-off).

Scenario – Every six months, three restore scenarios must be tested: backup data from the server at the switching centre.

Restore – Depending on the scenario, both full data is restored or specific data and date is restored.

Run tests – The specified tests must be conducted with each scenario.

Documents results – Results of the tests must be documented in the form of screenshots (bearing the date and time), compiled into a Word Document.

Store results – the results document must be stored and emailed to the IT manager. The file must be named using the following naming convention.

Scenariotested-yyymmdd-hhmm.doc

Review and sign-off – The IT manager must review the restore and test results within 30 days after receiving the email per above and file them (deemed signed-off).

1. B DISPOSAL OF IT SOLUTION

Purpose

To provide guidelines for proper and safe disposal of IT solutions which are no longer needed or have reached their end of useful life.

Scope

This procedure applies to all IT solutions used in the Department e.g. hardware and software. Leased and privately owned IT solutions used to perform official duties shall be affected by this procedure.

Process;

The asset owner responsibilities

- a) Call the IT unit to report the intention to dispose the hardware;
- b) Provide motivation for the intention to dispose the hardware;
- c) Identify data or information that still need to be retained; and
- d) Provide storage to store the data or information that still need to be retained.

RA

The IT unit responsibilities

- a) Attend to the received request to dispose the hardware;
- b) Transfer all the data or information still needed to another computer;
- c) Remove all the data and software in the computer earmarked for disposal;
and
- d) Provide a copy of the disposal assessment report to Asset management.

Asset management responsibilities

- a) Remove the hardware from the asset owner workstation.

1. C ACCESS CONTROL

Purpose

To control access into certain areas located within the interior of buildings. The purpose of an access control system is to provide quick, convenient access to those persons who are authorized, while at the same time, restricting access to unauthorized people.

Scope

This procedure is applicable to all IT solutions located in the Department premises. Various forms and systems are used as control measures to ensure effective access control measures. Forms are available from the IT unit and

Pwrt.mpu.gov.za/roads/systems.htm

Process;

Available forms include

- a) Access to email;
- b) Access to internet;
- c) Access to computer network; and
- d) Change of password.

RA

Access to email procedure

- a) Complete the email access form;
- b) Submit completed form to the IT unit;
- c) Check with the IT unit for application progress;
- d) Receive an email address and password; and
- e) Change default password.

Access to Network Access Procedure

- a) Complete the network access form;
- b) Submit completed form to the IT unit;
- c) Check with the IT unit for application progress;
- d) Receive a username and password; and
- e) Change default password.

Access to Internet Access Procedure

- a) Complete the Internet access form;
- b) Submit completed form to the IT unit;
- c) Check with the IT unit for application progress;
- d) Receive a username and password; and
- e) Change default password.

Change of password procedure

- a) Complete the password change form;
- b) Submit completed form to the IT unit;
- c) Receive a temporary password; and
- d) Change temporary password.

Handwritten mark

SOCIAL MEDIA GUIDELINES

Refer to Government Communication Policy as approved by Cabinet in October 2018.

RA