Department of Public, Works Roads and Transport

Mpumalanga Provincial Government

INFORMATION TECHNOLOGY (IT) SECURITY POLICY

Issue	05
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
DRP	: Disaster Recovery Plan
E-MAIL	: Electronic Mail
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 Organization for Standardization
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
WAN	: Wide Area Network
WWW	: World Wide Web

DEFINITIONS

Accounting Officer	Means	A person mentioned in section 36 of the Public Finance Management Act, 1999 (Act No. 1 of 1999) and includes any person acting as the Accounting Officer.
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 using Information Technology (IT) as an enabling tool;
Information Technology	Means	The processing of data via a computer/s. There are aspects of technology used to manage and support 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 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 confidentiality, availability, and integrity of systems and information;
Password	Means	A security code or PIN;
Server	Means	A 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	a person or organization responsible 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 (DPWR&T).

3rd party software	Means	Any application, tool, or program developed by a company that is not the original manufacturer of the device or primary software platform.
Private IT Solutions	Means	Bundle of services – whether they are software-based, or physical – that solve the information technology.
Barcode	Means	A visual, machine-readable representation of data using a pattern of parallel black bars and white spaces.
Data	Means	Raw, unprocessed facts and figures and figures that are given in a formalized, machine-readable format.
Information	Means	Data that has been processed to provide context and meaning, making it useful for a specific purpose, such as making decisions or answering questions.
Firewall	Means	A fundamental network security device that establishes a barrier between your trusted internal network and untrusted external networks.
Social media	Means	Websites, Apps and computer programs that allows users to create and share content or participate in virtual communities and social media

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 IT Security policy that will give guidance in establishing information security governance, practices, and procedures to protect its information technology assets.

2. OBJECTIVES

The objectives of this policy are to:

2.1. Promote information protection and security systems.

2.2. Protect information and information systems from loss, misuse, and damage.

2.3. Promote proper usage of IT solutions.

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)

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

5.1 Security

5.1.1 Security Management

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

5.1.1.2 The Department of Public Works, Roads and Transport is committed to safeguarding the confidentiality, integrity, and availability of its information assets throughout their entire life cycle—from creation and storage to use, sharing, archiving, and secure disposal. We ensure that all information is managed in compliance with applicable legislation, policies, and best practices to support effective service delivery, protect sensitive data, and enable informed decision-making. All employees and stakeholders are expected to uphold these principles and contribute to a secure information environment.

5.1.1.3 The Security Committee and Risk Management Committees responsible for all IT security related issues must be put in place. The committees must at least include representatives from the following 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
b) Management of the Department Security Program
c) Business Continuity and Disaster Recovery
d) IT Risk Management
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 Departmental IT resources are permitted.

5.1.2.6 All access to DPWRT network shall require a unique username and password.

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 Mpumalanga Provincial Treasury Security Policy shall govern all Wide Area Network (WAN) and Local Area Network (LAN) infrastructure. This policy ensures the continuous availability, integrity, and security of the Department's network infrastructure and data.

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 passphrases.

5.1.3.5 Administrator passwords shall be known only to designated IT personnel and must be securely stored to ensure the confidentiality and integrity of critical systems.

5.1.4 Unlicensed and Unauthorized Software

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

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

5.1.4.3 Officials are strictly prohibited from installing or using third-party software to process departmental data without prior consultation with the IT Unit or formal approval from the Accounting Officer. This measure ensures the integrity, security, and compliance of all departmental information systems.

5.1.5 Physical Security

5.1.5.1 The Minimum Information Security Standard (MISS) shall apply. 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.

5.1.5.3 Where feasible fire prevention standards and procedures shall be established and adhered to, in line with the Disaster Management Plan, to prevent fire from starting spontaneously due to negligence or because 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.

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 the servers hosting data and applications shall be 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 restricted or 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.

5.1.6.5 Servers data shall be backed up in accordance with the DPWRT backup guidelines / procedures.

5.1.7 Workstation Security

5.1.7.1 All departmental computers shall be barcoded to confirm official ownership and facilitate asset management. The IT Unit shall provide technical support exclusively to barcoded departmental machines. Support for newly acquired computers will be provided upon verification of purchase and pending barcode registration

5.1.7.2 All workstations shall be 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.

5.1.7.3 All workstations shall be loaded and protected by the latest approved Anti-Virus software.

5.1.7.4 It is the responsibility of the workstation user to ensure that appropriate security measures and practices are adhered to.

5.1.7.5 Users shall not leave their workstations unattended while accessing or processing information without appropriate protection like password protected screen savers.

5.1.7.6 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.

5.1.7.7 Users shall not share workstation passwords and user accounts with anyone.

5.1.7.8 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.

5.1.7.9 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.

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.

5.1.8.4 Changing of Given Passwords.

5.1.8.4.1 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.

5.1.8.4.2 All passwords reset requests must be submitted using the official Password Reset Form. The IT Unit will only process requests that are completed and submitted by the individual user. Requests made on behalf

of another user will not be accepted under any circumstances to ensure security and accountability.

5.1.8.5 Account Lockout.

A user's account will be automatically locked after three consecutive unsuccessful login attempts. Only the IT Unit is authorized to unlock user accounts to maintain system security and prevent unauthorized access. Requests made on behalf of another user will not be accepted under any circumstances to ensure security and accountability.

5.1.8.6 Identification.

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

5.1.9 Encryption

5.1.9.1 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.

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

5.1.10 Security and Protection of Records

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

5.1.11 Third Party Connections Security

5.1.11.1 Departmental information shall not be accessed, processed, or transmitted using internet café networks or privately owned Wi-Fi connections. These networks are not managed or secured by the Department and may pose significant risks to the confidentiality, integrity, and availability of sensitive departmental data. All officials must use approved and secure departmental networks when handling official information to ensure compliance with information security standards.

5.1.11.2 To protect the confidentiality, integrity, and sovereignty of departmental data, only Microsoft AI tools are authorized for uploading and processing

information related to the Department of Public Works, Roads and Transport. The use of any other AI platforms or online tools that require users to upload departmental data to external websites is strictly prohibited. Such tools pose significant data security risks, including unauthorized access, data leakage, and loss of control over sensitive information. All staff must ensure that departmental data is processed exclusively within approved and secure environments.

5.1.11.3 Third Party persons shall have approval of the Accounting Officer to access DPWRT Network. All approved changes shall be monitored to ensure that they are implemented according to specification.

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

5.1.12 Firewall (as per the MOU with MPT)

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 other official is allowed to temper with IT solutions.

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.

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 All officials must promptly report any actual or suspected information security incidents—including data breaches, unauthorized access, malware infections, or loss of departmental data or devices—to the IT Unit. Timely reporting is essential to minimize risk, contain potential damage, and ensure appropriate corrective actions are taken

5.2.4.2 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.

5.2.4.3 An Incident include the following:

a) Network attacks.
b) Denial of services.
c) Theft.
d) Infrastructure compromise.
e) Virus infections availability.
f) Integrity compromise.
g) Fraud.
h) Illegal activity.
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 Departmental information shall not be transmitted using non-official email services including personal email platforms. These services security controls may compromise sensitive departmental data and may expose information to unauthorized access or compromise. All official communication involving departmental data must be conducted through approved and secure departmental email systems.

5.2.6.2 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 the property of MPT.

5.2.6.3 MPT 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.

5.2.6.4 Misrepresenting, obscuring, suppressing or replacing the identity of a user on an electronic communications system is forbidden. The username, 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.

5.2.6.5 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.

5.2.6.6 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.

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 MPT internal Web proxy server before gaining access to the Internet. This authentication process shall be achieved by logging on to the Internet via username and password system.

5.2.7.5 To protect MPT 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 MPT 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 MPT 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.

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 responsible for the effective and efficient implementation of this policy as part of internal controls within the Department.

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 every 5 years or as and when there is a need to factor in changes in legal framework 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 15/07/2026

ANNEXURE 1: PROCEDURES

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 recovery (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).

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.
d) Provide storage to store the data or information that still need to be retained.

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.
d) Provide a copy of the disposal assessment report to Asset management.

Asset management responsibilities

Remove the hardware from the asset owner workstation.

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.qov.za/roads/systems.htm.

Process

Available forms include

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

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.
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.
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.
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.
d) Change temporary password.

ANNEXURE 2: SOCIAL MEDIA GUIDELINES

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