



LIMPOPO

PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT
OF
PUBLIC WORKS

Policy Name	Information Technology
The revision/ version of the Policy	01
Domain	ICT

TABLE OF CONTENTS

1. ACRONYMS AND ABBREVIATIONS3

2. INTRODUCTION4

3. PURPOSE AND OBJECTIVES4

4. AUTHORITY OF POLICY4

5. LEGAL FRAMEWORK4

6. SCOPE OF APPLICATION45

7. DEFINITIONS5

8. POLICY PRONOUNCEMENT56

8.1 USER AWARENESS56

8.2 POLICY PROVISIONS/RESPONSIBILITIES6

9. INFORMATION TECHNOLOGY AND SYSTEMS SECURITY POLICY6

10. IT PREMISES ACCESS CONTROL6

11. IT NETWORK INFRASTRUCTURE SECURITY POLICY AND/OR ACCESS CONTROL67

12. PASSWORD POLICY8

13. IT INFRASTRUCTURE REQUIREMENTS8

14. FACILITY CONSTRUCTION REQUIREMENTS9

15. SOFTWARE USAGE AND LICENSING POLICY9

16. E-MAIL POLICY9

17. INTERNET AND INTRANET POLICY10

18. ANTI-CYBER CRIME POLICY11

19. ENCRYPTION POLICY1112

20. ANTIVIRUS POLICY1112

21. PRINTING POLICY12

22. IT BACKUP AND ARCHIVAL POLICY12

23. DETECTION AND RESPONSE TO IT INCIDENTS1213

24. PROTECTION OF ELECTRONIC DATE13

25. IT EQUIPMENT/HARDWARE/INFRASTRUCTURE POLICY13

26. IT SERVICE/HELPDESK POLICY1314

27. IT ASSETS DISPOSAL POLICY14

28. IT PROCUREMENT POLICY14

29. DEFAULT14

30. INCEPTION DATE14

31. TERMINATION AND REVIEW1415



1. ACRONYMS AND ABBREVIATIONS

LDPW	Limpopo Department of Public works
IT	Information Technology
FTP	File Transfer Protocol
PDA	Personal digital assistant
HOD	Head of Department
CD	Compact disc
LAN	Local Area Network
PC	Personal Computer
TCP/IP	Transmission Control Protocol/Internet protocol
IT & IS	Information Technology & Information System

A handwritten signature in black ink, appearing to be a stylized name, located in the lower right quadrant of the page.

2. INTRODUCTION

For over twenty years Information Technology Security has held that confidentiality, integrity and availability are the core principles of Information Technology Security. Information Technology Security which refers to protection of information assets protects information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction. We have moved in an information age, in which the gathering, use, development and distribution of information in electronic form dominate economic activities, and wealth is tied up in electronic information. LDPW seeks to provide appropriate access to information among its IT Users/Departmental personnel, clients and stakeholders.

This policy shall not only cover the security of information itself, but also computer software, hardware, networks and infrastructure supporting information systems.

3. PURPOSE AND OBJECTIVES

The purpose of this document is to guide the use, procedures, principles, norms and standards, rules, regulations for the protection, and preservation of all electronic information, which is generated by, owned by, or otherwise in possession of LDPW.

More government Departments this day and age are moving away from the traditionally paper based Departmental standards, to a more automated and electronic one. There are numerous case studies that demonstrate the benefit of such a move, which range from speed, cost reduction, less inventory, better quality, less theft, space saving, control and transparency. LDPW, aspiring to become the leader in the provision and management of provincial government land and building is adopting this thinking.

4. AUTHORITY OF POLICY

This policy is authorized and issued by the Executive LEGAL FRAMEWORK

- The constitution of the republic of south Africa act, 1996 (Act no. 108 of 1996)
- White paper on transforming public service 1997
- Kings reports III
- Electronic transaction and communication Act,2002(Act no3 25 of 2002)
- Minimum information security standard
- Provincial E-government strategy
- Public Service Act,1994(Act no103 of 1994) as amended
- Public Service regulations 2001
- Public Finance Management Act,1999 (Act no1 of 1999)as amended by Public finance Management Act,1999 (Act no29 of 1999)
- Minimum interoperability standard
- Protection of information Act ,1982 (Act no. of 1982)
- National Information Security Regulations
- SITA amendment Act,2002(Act no 38 of 2002)
- Electronic Communications Security Act, 2002(Act no.68 of 2002)
- Public Service IT Policy Framework of February 2001.

5. SCOPE OF APPLICATION

This policy is applicable to all personnel, contractors, part-time and temporary workers of LDPW and those that are employed by others to perform work on LDPW premises or granted access to Department's

information or IT equipment, are covered by this policy and its underlying principles. IT policy is intended to support, protect, control and manage information resources of LDPW.

DEFINITIONS

Terms	Definitions
Simple Mail Transfer Protocol	It's a TCP/IP protocol used in sending and receiving of e-mail across the Internet.
Spam	Also known as "bulk e-mail" or "junk e-mail," is a subset of spam that involves nearly identical messages sent to numerous recipients by e-mail.
Compact Disc	It's an optical disc used to store digital data, originally developed for storing digital audio.
Personal digital assistant	an electronic device which can include some of the functionality of a computer, a cell phone, a music player, and a camera
Modem	It's a network device that modulates outgoing digital signals from a computer or other digital device to analog signals for a conventional copper twisted pair telephone line and demodulates the incoming analog signal and converts it to a digital signal for the digital device
Router	It's a device or, in some cases, software in a computer, that determines the next network point to which a packet should be forwarded toward its destination.

6. POLICY PRONOUNCEMENT

8.1 User Awareness

Departmental Officials are encouraged to familiarize themselves with the Departmental IT policy as well as their roles and responsibilities. Improved awareness of IT policy issues and procedures does not only reduce the risk of information accidents, but also increases the likelihood of suspicious activities being reported and preventative measures being implemented.

8.2 Policy Provisions/Responsibilities

Government Information Technology Directorate is responsible for the implementation and update of IT policy document, and upon approval an e-mail shall be sent out to advise IT Users/Departmental personnel about the amendments and updates made to the document. Copies of these policies shall be hosted on the departmental intranet. Human Resource Management Directorate shall ensure that newly appointed personnel are required to agree that they shall conform to the policies, standards and codes of practice.

All IT Users/Departmental IT Users/personnel members of the Department shall be personally responsible for understanding, following Information Technology Policies, and shall be personally accountable for the consequences of any security violation resulting from their failure to observe such policies. The Department shall identify and provide appropriate IT policy awareness tools to support this process.

Information Technology and Systems Security Policy

IT Directorate shall:

- 9.1. Provide all permanent or contract or temporary IT Users/Departmental personnel with Information Technology Security awareness tools to enhance awareness and educate them regarding the range of threats and the appropriate safeguards.
- 9.2. Provide appropriate Information Technology Security Policies .
- 9.3. Provide regular and relevant Information Technology Security awareness communications to all IT Users/Departmental personnel by various means, such as electronic updates, briefings, newsletters, etc.
- 9.4. Ensure individuals entrusted with the responsibility for configuring and maintaining Information Technology Security safeguards have the relevant skills and competencies.
- 9.5. Review user access rights regularly.
- 9.6. Provide training to all Users of new systems to ensure that their use is both efficient and does not compromise Information Technology Security.
- 9.7. Ensure that external Service Providers abide by the Departmental Information Technology Security policies.

IT Premises Access Control

This refers to IT server room, storage, data centres, computer lab and any other sensitive IT premises.

IT Directorate shall:

- 10.1. Ensure that physical access to IT high security areas are controlled with appropriate identification techniques, recorded and is approved by management.
- 10.2. Ensure that IT premises are safeguarded against unlawful and unauthorized physical intrusion.

Departmental IT Users/personnel shall:

- 10.3. Comply with the Information Technology Security Policies of the Department. Any Information Technology Security incidents resulting from non-compliance shall be referred for investigation and may result in corrective measures being instituted against the perpetrator.

IT Network Infrastructure Security Policy and/or Access Control

IT Directorate shall:

- 11.1. Ensure that the network is designed and configured to deliver high performance and reliability to meet the needs of the business whilst providing a high degree of access control and is sufficiently safeguarded against unauthorized network intrusion.
- 11.2. Ensure that all requests to access Departmental IT infrastructure is documented and approved via a formal process and procedure.
- 11.3. Ensure that all Users' requests to access Departmental IT infrastructure are approved by Users' immediate supervisors or delegated personnel.
- 11.4. Ensure termination and/or modification of Users' account on Departmental IT infrastructure is approved by delegated personnel.
- 11.5. Provide User access as per User job responsibilities or Departmental business activities or segregation of duties. E.g. Access will be issued as per job profile, there should be clear distinction between the system administrator, system user, etc.
- 11.6. Periodically check if User access is commensurate with their current job responsibilities.
- 11.7. Ensure that intranet servers, electronic bulletin boards, local area networks, modem connections to existing internal networks, or other multi-user systems for communicating information are not established without the specific approval of LDPW' IT Directorate.
- 11.8. Ensure that suitably qualified Officials manage the Department's network, and preserve its integrity in collaboration with the nominated individual system owners.
- 11.9. Periodically review systems administrator activities.
- 11.10. No unauthorized equipment shall be connected to any network infrastructure within LDPW without approval of LDPW' IT Directorate.
- 11.11. Ensure that remote access to the Department's network and resources is approved and monitored.
- 11.12. Ensure that network users connected via TCP/IP are not simultaneously connected via a modem to the Internet or any other external TCP/IP network without explicit management authorization and unless the appropriate TCP/IP commands are entered which prevents intruders from using the workstation as a pathway into the internal network.
- 11.13. Ensure that in-house production information systems, such as server, are not directly connected to the Internet; instead these systems will connect with an application server, a database server, or some other intermediate computer that is dedicated to Internet business activity.
- 11.14. Ensure that all web servers accessible via the Internet are protected by a router or firewall approved by LDPW' IT Directorate.
- 11.15. Ensure that access control to Departmental applications is configured and reviewed on a regular basis. E.g. recording of access violation.

Departmental IT Users/personnel shall:

- 11.16. Not establish intranet servers, electronic bulletin boards, local area networks, modem connections to existing internal networks, or other multi-user systems for communicating information without the specific approval of LDPW' IT Directorate.
- 11.17. Not connect via TCP/IP and simultaneously connected via a modem to the Internet or any other external TCP/IP network without explicit management authorization and unless the appropriate TCP/IP commands are entered which prevents intruders from using the workstation as a pathway into the internal network
- 11.18. Not allow anonymous FTP, or other unauthenticated access to program or data files on their workstation.
- 11.19. Not establish direct connection between LDPW' systems and computers at external Departments (tunnels or virtual private networks) via the Internet or any other public network unless authorized to do so via a formal approval.
- 11.20. Not make arrangements for installation of voice or data lines with any carrier, without consultation and approval from the LDPW' IT Directorate.



Password Policy

A Password is a series of characters that enables someone to access a file, computer or program and is a key control that prevents unauthorized Users from accessing personnel information.

Departmental IT Users/personnel shall:

- 12.1. Own protection of LDPW' resources' by keeping his/her password including other authentication mechanisms secret and not share it with anyone else.
- 12.2. Regardless of the circumstances never share or reveal passwords to anyone.
- 12.3. Choose passwords for computer and networks that conform to best practice and meet the following standards: - A combination of 6 alpha numeric characters with at least on capital letter character.
- 12.4. Be responsible for all activity performed with their personal User-IDs.
- 12.5. Not store password in readable form in batch files, automatic login scripts, software macros, terminal function keys, in computers without access control, or in other locations where unauthorized persons might discover or use them.
- 12.6. Change all passwords immediately if they are suspected of being disclosed to unauthorized parties.
- 12.7. Not load non-approved screen savers onto the Departmental PC's, laptops and workstations.
- 12.8. Not leave their screen unattended but ensure that they firstly lock access to their workstation or log off.
- 12.9. Change password as and when required by IT Directorate.

IT Directorate shall:

- 12.10. Create User passwords for both computer and network using an approved procedure modeled on best practice.
- 12.11. Change all vendor-supplied default passwords before any computer or communications system is used.
- 12.12. Change all passwords immediately if they are suspected of being disclosed to unauthorized parties.
- 12.13. Implement procedures/mechanisms to enforce password controls adhering to best practice.
- 12.14. Ensure that screen savers are activated within set limits of user inactivity and should be password controlled.
- 12.15. Periodically reset Users' passwords. Such activity shall be automated and acceptable history of user account activity logs kept.
- 12.16. Implement passwords reset procedures with prescribed security checks to authenticate the validity if the user.
- 12.17. Establish and enforce software lockout mechanisms in case of failed attempted log inns.
- 12.18. Review Users/Departmental personnel's continued Network access rights.
- 12.19. Ensure password resets are recorded.
- 12.20. Ensure an authentication mechanism be utilised to verify the authenticity of the Official requesting a password reset.

IT Infrastructure Requirements

IT Directorate shall:

- 13.1. Choose sites to store or place computers and to store data and protect them from physical intrusion, theft, fire, flood, excessive ambient temperature or humidity and other hazards.
- 13.2. Obtain environmental storage requirements from the IT hardware manufacturer and implement them. And the physical security measures adopted, should take into cognizance the value of the hardware, the sensitivity of personnel data and the required level of service resilience.



Facility Construction Requirements

Department of Public Work/Business Units shall:

- 14.1. Ensure that development of new Departmental facility construction plan, extension of an existing facility plan and renovations of facilities plans incorporate the required IT plans, architecture and sufficient funds exist to support the required ICT deliverables. NB. Any costs incurred for damage(s) to ICT infrastructure due to unsanctioned facilities construction/modification may lead to the responsible official being subjected to corrective action.

Software Usage and Licensing Policy

- All software applications developed for the use by LDPW by 3rd parties becomes the property of LDPW.
- Software (including all copies if any) purchased by LDPW shall be returned to LDPW upon termination of employment or contract.
- To comply with legislation and to ensure ongoing vendor support, the terms and conditions of all End User License Agreements are to be strictly adhered to.

IT Directorate shall:

- 15.1. Only install licensed and authorized software licenses on LDPW' equipment.
- 15.2. Ensure that all software licenses certificates and CD are kept for renewal purpose and reference by IT Directorate.
- 15.3. Remove unauthorized software from the departmental IT equipment.
- 15.4. Screen all software and files downloaded from non-Departmental source via the Internet (or any other public network) with the LDPW' approved proxies, virus detection software and other mechanisms before being executed.
- 15.5. Restrict installation of software by Users using appropriate controls based on user access rights.

Departmental IT Users/personnel shall:

- 15.6. Not install any software without prior IT Directorate's approval.
- 15.7. Not copy and/or distribute departmental software.
- 15.8. Not download, install and/or using evaluation, public domain, freeware and shareware without prior permission from IT Directorate.

IT Directorate shall:

- 15.9. Periodically audit LDPW' IT equipment and software license use.

E-Mail Policy

E-mail, short for electronic mail and often abbreviated to *e-mail*, *email* or simply *mail*, is a store and forward method of composing, sending, storing, and receiving messages over electronic communication systems. It is the property of LDPW and should be used responsibly and shall be used for business purposes only.

IT Directorate shall:

- 16.1. Secure email infrastructure.
- 16.2. Ensure that incoming e-mail are treated with the utmost care due to its inherent Information Technology Security risks. LDPW reserves the rights to review E-mails use at any time without notice where suspected abuse and activity is noted.
- 16.3. Ensure backup and data retention of e-mail in line with legal and business requirements.
- 16.4. Implement email-filtering systems.
- 16.5. Ensure that every outgoing e-mail message contain this disclaimer at the end e.g. "All views expressed *herein are the views of the author and do not reflect the views of Public works unless specifically stated otherwise. The information is intended only for the person or entity to which it*



is addressed and may contain confidential and /or privileged material .Any review, retransmission, dissemination or other use of ,or taking action of any action in reliance upon ,this information by persons or entities other than those intended recipient/s is prohibited. If you received this message in error, please contact the sender and delete the material from your computer” This disclaimer shall be appended electronically to all outgoing emails by the Departments’ email servers.

Departmental IT Users/personnel shall:

- 16.6. Not open e-mail suspect email file attachments.
- 16.7. Not forward confidential, proprietary information to third parties.
- 16.8. Regularly check his/her mailbox for received messages.
- 16.9. Ensure that the content of their messages cannot be misconstrued and that there is nothing unlawful about the transmission or content of the message.
- 16.10. Not transmit e-mail messages containing but not limited to the following:
 - Offensive, defamatory, discriminatory or harassing material;
 - Sexually explicit or other offensive images or jokes;
 - Unlicensed copyright materials;
 - Non-business related video and image files;
 - Any messages which would be deemed unlawful pursuant to the applicable law of any governing jurisdiction;
 - Advertisements;
 - Chain letters
- 16.11. Compress E-mail messages large than 1 MB using the applicable and Departmental utilities e.g. WinZip, etc.
- 16.12. Not use email for personal gain e.g. creating or participating in pyramid schemes.
- 16.13. Not use an e-mail account assigned to another employee to either send or receive messages.
- 16.14. Treat received unwanted or unsolicited e-mail(also known as SPAM) with caution and not respond to it.
- 16.15. Ensure that all messages have appropriate subject title, and no messages are to be sent out without the subject line.
- 16.16. Not distribution to other IT Users/Departmental personnel of offensive 'joke of the day' e-mails.
Not mass mail email to all users unless authorized to do so in writing.

Internet and Intranet Policy

Internet is a worldwide system of computer networks - a network of networks in which Users at any one computer can, if they have permission, get information. The possible loss of privacy or leakage of information and misuse of Internet must be safeguarded. LDPW’ intranet and internal LAN systems are for the exclusive use of authorized LDPW personnel and authorized users. Automatic access to the Internet is not a right.

IT Directorate shall:Provide Internet to all LDPW personnel and contractors upon approval through approved network access procedures.

Revoke access if it is found that a user misuses the facility. Excessive 'surfing' of web sites during business hours for personal use is regarded as spending more than one hour of an eight-hour shift on the Internet.Use filters/proxies and other techniques whenever possible to restrict access to inappropriate information on the Internet by IT Users/Departmental personnel. Review and report attempted access violations on a regular basis.

Ensure that Internet access is safeguarded from malicious external intrusion by deploying intrusion detection systems.(e.g. Firewalls)

Departmental IT Users/personnel shall:

Apply for access for Internet using established procedures. Approval from relevant managers is required.



Not advertise, promote, present, or otherwise make statements about Public works' products and services on Internet forum such as mailing lists, news groups, and chat sessions without the prior approval of LDPW' Communication Directorate.

Not use the available Internet for:

Viewing and/or downloading of pornographic or obscene material of any nature;

The dissemination of material that advocates hatred and/or conflict or which causes discomfort or embarrassment to the Department or their fellow colleagues by way of discrimination based on race, ethnic group, gender, religion, sexual orientation, age and/or material that propagates sexual harassment;

The dissemination of material supporting any petition, or advertising any services not specifically authorized in writing by the Department ;

The transmission of any message of an abusive and defamatory nature of anyone either internally or externally;

The use of Internet, intranet and email facilities for any purpose whatsoever not connected to or forming an integral part of Department's operation or business.

Web sites that advocate any illegal activity.

Playing games and using 'chat rooms'.

Subscribing and contributing to news groups using the corporate Internet address and signature.

Sending and receiving personal correspondence by e-mail, the volume and content of which is deemed as excessive and / or inappropriate. Consider all information taken off Internet as suspect until confirmed by relevant source. Non-Departmental computers are prohibited from establishing connection to LDPW' networks without specific and prior written permission from IT Directorate. Not use network probing against any LDPW Internet infrastructure and servers.

18. Anti-Cyber Crime Policy

IT Directorate shall:

Ensure access control standards and data classification standards are periodically reviewed whilst maintained at all times in order to reduce the incidence and possibility of attacks.

Ensure priority in minimizing the opportunities for cyber crime attacks on the Department's systems and information through a combination of technical access controls and robust procedures.

Conduct awareness sessions encouraging IT Users/Departmental personnel vigilance on cyber crime.

19. Encryption Policy

IT Directorate shall:

Under dual control perform the management of electronic keys to control both the encryption and decryption of sensitive messages.

Ensure that remote access control procedures provide adequate safeguards through robust identification, authentication and encryption techniques.

Ensure that where appropriate, sensitive or confidential information or data is always transmitted in encrypted form. Prior to transmission, consideration shall always be given to the procedures to be used between the sending and recipient parties and any possible legal issues from using encryption techniques.

20. Antivirus Policy

The threat posed by the infiltration of a virus is high, as is the risk to the Department's systems and data files.



Departmental IT Users/personnel shall:
Not install unauthorized antivirus software on Departmental equipment.

IT Directorate shall:
Deploy without Antivirus software to all relevant ICT infrastructure, with regular virus definition updates and scanning.
Regularly review and monitor virus incident response.

21. Printing Policy

LDPW printing equipment shall be utilized for official purposes only.

Departmental IT Users/personnel shall:
Not use Departmental IT printing facilities for personal use.
Not print internal documents in colour except special presentations to the external stakeholders, due to the prohibitive costs of colour printing.

IT Directorate shall:
Restrict colour printing to documents/proposals to be presented to the client/shareholder/board.
Ensure that use of desktop printers is minimized.
Establish centralized printing facilities.

22. IT Backup and Archival Policy

The archiving of electronic data shall take place with due consideration for legal, regulatory and business issues with liaison between technical and business IT Users/Departmental personnel.

Departmental IT Users/personnel shall:
Save all electronic data in the mapped network drive.

IT Directorate shall:
Ensure that adequate backups of electronic data are taken at regular intervals.
Implement ICT disaster recovery, ICT business continuity systems and procedures.
Ensure that the frequency of backup operations and procedures for recovery meet the needs of the business.
Ensure that the archiving of electronic data files shall reflect the needs of the business and also any legal and regulatory requirements.

23. Detection and Response to IT incidents

Departmental IT Users/personnel shall immediately notify all identified or suspected Information Technology Security weaknesses and/or breaches to the Information Technology Security Officer.

IT Directorate shall:
22.1. Ensure that IT incident and risk register is in place.
Review IT incident and risk register on a regular basis.
Regularly monitored the use of information systems with all unexpected events recorded and investigated.



24. Protection of electronic data

Notwithstanding the Department's respect for employee's privacy in the workplace, it reserves the right to have access to all electronic data created and stored on the Department's systems.

Departmental IT Users/personnel shall:

Ensure that only authorized persons may access sensitive or confidential data on projects owned or managed by the Department or its personnel.

Ensure that LDPW' confidential information and material are locked in a safe environment when not in use, this includes information recorded on portable media such as memory sticks, compact disks (CDs), notebooks, laptops, PDAs etc. to protect the information against theft and unauthorized access.

IT Directorate shall:

Ensure that authorized Users of information systems manage the creation, storage, amendment, copying and deletion / destruction of data files in a manner which safeguards and protects the confidentiality, integrity and availability of such files.

Ensure that the use of shared data repositories, are used in accordance with appropriate software security controls and measures to manage the access to the information.

25. IT Equipment/Hardware/Infrastructure Policy

The following list outlines the IT assets that will be affected, but is not limited to the following:

- Computers (e.g. Desktops, laptops, Tablet pc's, etc...);
- Peripheral IT equipment (e.g. printers, scanners, data projectors, flash disk, etc...)
- Network infrastructure (e.g. hubs, switches, routers, cabling, servers, etc...)
- Personally owned IT equipment that is in the Departmental premises and/or access Departmental network

Departmental IT Users/personnel shall:

Ensure that all notebooks are fitted with a physical lock cable, which must be hooked to an immovable object to make it difficult to steal.

Not use the Department's ICT infrastructure for private business.

Safeguard ICT infrastructure in their possession.

Regardless of location (e.g. office, car, hotel and plain) have the responsibility to appropriately protect the Departmental ICT assets.

Be held fully responsible for the ICT equipment loss, unless it can be determined that it was not at fault.

Report IT equipment or LDPW' confidential information lost or stolen to Risk Management Services, IT, Law enforcement agencies (SAPS) and the head of his/her Directorate within twenty-four hours of discovery thereof.

IT Directorate shall:

Issue portable computers in accordance with set standards.

Not provide IT support on personally owned IT equipment.

26. IT Service/Helpdesk Policy

Departmental IT Users/personnel shall:

Log desktop related call to relevant call centres using approved procedures.

Escalate unresolved calls or desktop support dissatisfactions to IT Directorate in writing.

IT Directorate shall:

Manage applicable service level agreements for services rendered by contracted service providers.

27.IT Assets Disposal Policy

IT Directorate shall:

- Conduct regular ICT infrastructure lifespan reviews and or recommend the disposal of earmarked IT assets to Office of the Chief Financial Officer.
- Ensure compliance to the acceptable IT infrastructure disposal norms and standards
- Adhere to LDPW Assets management policy.

IT Technical or Infrastructure Officer shall:

Archive data from the obsolete or redundant IT equipment and destroy the information using acceptable norms and standards.

28. IT Procurement Policy

IT procurement shall be channeled through the Office of the Chief Financial Officer utilizing Treasury regulations and SITA contracts.

29.Default

Non –Compliance with the principles as described in this policy document may result in corrective action including disciplinary action.

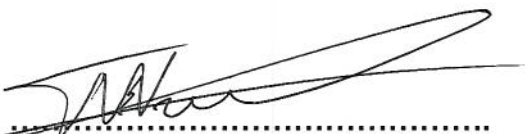
30. Inception Date

The inception date of this policy will be effective from the date of approval by the Executive Authority.

31. Termination and Review

This policy will be reviewed when there are new developments in terms of legislation.

APPROVED



.....

EXECUTIVE AUTHORITY

25/07/13
.....
DATE