



LIMPOPO

PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

PROVINCIAL TREASURY

LIMPOPO PROVINCIAL TREASURY

IT POLICY

TABLE OF CONTENT

Item no	Description	Page no
1	Preamble	3
2	Applicable Legal Framework	3
3	Objectives	3
4	Scope	3
5	Policy provisions/ responsibilities	4
6	Definitions	4
7	Policy principles	6
8	Policy control	21
9	Effective Date	21
10	Ratification	21

1. PREAMBLE

The IT Policy will outline the principles and standards which determine acceptable use of the computing resources of the Limpopo Provincial Treasury (LPT). The primary aim of this policy document is to balance the proper and efficient business of the computing resources against the need for protection of the systems, service and information that makes up those resources

2. APPLICABLE LEGAL FRAMEWORK

This policy has been developed within the following applicable 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 II
- Electronic Transaction & Communication Act, 2002 (Act no.3 25 of 2002)
- Minimum Information Security Standard
- Provincial E-Government Strategy
- Public Service Act, 1994 (Act no.103 of 1994) as amended
- Public Service Regulations 2001
- Public Finance Management Act, 1999 (Act no.1 of 1999) as amended by Public Finance Management Act, 1999 (Act no.29 of 1999)
- Minimum Interoperability Standard
- Protection of Information Act, 1982 (Act no. 84 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

3. OBJECTIVES

- The purpose of this policy is to outline the efficient use of departmental IT systems and to curb unnecessary usage of computing resources of LPT.
- The IT policy will ensure the balance between the proper and efficient business of the computing resources against the need for protection of the systems, service and information that makes up those resources

4. SCOPE

This policy applies to all employees as well as contractors and any other individual conducting business or using LPT IT infrastructure.

5. **POLICY PROVISIONS/ RESPONSIBILITIES**

- Non-compliance with the principles as described in this policy document may result in disciplinary action, possibly including dismissal. It is therefore vital that all employees and contractors to LPT who utilize the systems are made aware of the policy.
- The Government Information Technology directorate is responsible for the implementation and updating the IT policy document, and upon approval an e-mail will be sent out to advising everyone about the amendments and updates made to the document.
- Human Resource Management section will ensure that newly appointed employees are required to agree that they will conform to these standards and codes of practice.

6. **DEFINITIONS**

ACRONYM	DESCRIPTION
LPT	Limpopo Provincial Treasury
SITA	State Information Technology Agency
E-mail	Electronic mail communications system that allows people to send and receive mail via computer networks.
dial-up service	Gaining access to the Internet from a stand alone computer through a direct telephone line by means of a modem.
down load	To transfer data or programs from a computer which is on a network other than one's own local area network to one's own computer, or from a computer which is on one' own local area network such a file server to one's own computer.
Internet Content Filter	It is a piece of software that, once installed on a computer, act as a censor while you browse the World wide Web
Encryption	Encoding or obscuring data according to some rule, procedure or algorithm agreed upon by trusted parties both of whom have the key to the algorithm.
Website	A page on a web site (that is, a computer that has a distinct address on the Internet) on the Internet where information is placed by a person or organisation that can be accessed by anyone connected to the Internet.

ACRONYM	DESCRIPTION
hyper text	A computer program that provides multiple pathways through text that enable the user to link related items of text together or retrieve linked cross-references in a random access manner.
Internet browser	Client software for viewing hyper text/ hyper media documents on the World Wide Web.
Internet service provider	A company which provides clients with authorisation and connection to the Internet.
Modem	A device used to translate digital signals from a computer into analogue signals used by a telephone line and vice versa.

7. POLICY PRINCIPLES

7.1 ACCEPTABLE USE OF E-MAIL

Electronic Mail (Email) functions like ordinary mail. The sender writes an electronic letter and may add, if needed, enclosures such as text documents, graphics or spreadsheets. The sender then 'posts' the message by adding the recipient's Email address, often selected from an electronic address book. Email uses resources that can be distributed over several data networks. The user's conduct contributes to whether or not the availability and confidentiality of the system is ensured.

- Incidental private use of e-mail facility is permitted but this is subject to strict control and abuse of this privilege may be regarded as misconduct.
- All Emails created, sent, forwarded, stored or printed are the property of LPT. LPT reserves the right to inspect the Emails at any time without notice.
- Through using Email you are deemed to have read, understood and agreed to the IT Policy document relating to e-mail systems contained within this policy.
- All users of e-mail system are not as matter of course allowed to forward confidential, proprietary information to third parties. Users will be expected to delete any such information received from the e-mail system after having been read.
- Email users are expected immediately to detach, and scan any email attachment which is unsolicited or of unknown origin or alternately delete it.
- It is the responsibility of the sender to ensure that the intended recipient of the message has suitable tools to work on any enclosed document(s).
- Unnecessarily distribution of email messages to groups and distribution list is prohibited.
- It is the responsibility of every e-mail user to check his/her mailbox regularly for received messages.
- All email users are responsible for ensuring that the content of their messages cannot be misconstrued and that there is nothing unlawful about the transmission or content of the message.
- Certain disclaimers may be required for messages requiring confidentiality, legal privilege etc.

- It is prohibited to display or transmit email messages containing but not limited to the following:
 - offensive, defamatory, discriminatory or harassing material;
 - sexually explicit or other offensive images or jokes;
 - unlicensed copyright material;
 - non- business related video and image files;
 - any message which would be deemed unlawful pursuant to the applicable law of any governing jurisdiction;
 - advertisements;
 - chain letters.
- email messages larger than 1MB must be compressed using the applicable and departmental utilities e.g. Winzip, Winrar etc.
- Sending of large number of email messages to a single address is prohibited, as it may disable the destination mailbox.
- The email system is the property of LPT and should be used responsibly. Users are not allowed to use the e-mail system for gain e.g. creating or participating in pyramid schemes.
- When using electronic mail to communicate with people on the Internet, users must not activate the Auto-Reply facility function such as “Out of the Office message option”.
- Employees shall not use an electronic mail account assigned to another individual to either send or receive messages.
- Employees must regularly move important information from electronic mail message files to word processing documents, databases, and other files, as email messages may be erased periodically, either accidentally or as part of normal archiving and file maintenance functions.
- If employees receive unwanted and unsolicited email (also known as SPAM), they must refrain from responding directly to the sender.
- Employees shall not employ scanned versions of hand-rendered signatures to give the impression that an electronic mail message or other electronic communications were signed by the sender.
- An automatic function will be activated to delete email messages from the server that are older than one calendar month.
- It is the responsibility of an individual employee to manage his/her own Email download once she/he has downloaded it.

- Important email attachments must be saved in an appropriate folder within the “My Documents” folder and saved to a network server for backup.
- All messages are required to have appropriate subject title, and no message must be sent out without the subject line.
- Every outgoing email message must contain a disclaimer at the end e.g. *“All views expressed herein are the views of the author and do not reflect the views of the Provincial Treasury 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.”*

7.2 ACCEPTABLE USE OF INTERNET

The department’s information, computing assets, and corporate image on the Internet are critical to our success, and as a result, must be protected from loss, modification or destruction.

The Internet is used to connect with our customers, suppliers and other organisations. It is important to remember the internet is used by millions of people worldwide and unprotected information sent across the internet may well be read by any number of unknown people.

The possible loss of privacy or leakage of information about LPT is what mainly informs it to development a policy document on the use of the internet facility.

- Only those employees and users who have received management approval may access the Internet via LPT’s facilities. Automatic access to the Internet is not a right, and access can be revoked if it is found that misuse of the facility is occurring.
- Internet access will be provided on application to all LPT employees and contractors with valid Persal/ID numbers and those with access to a computer.

- Whenever an employee posts a message to an Internet discussion group, an electronic bulletin board, or another public information system, the message shall be accompanied by words clearly indicating that the comments do not necessarily represent the position of LPT.
- Unless expressly authorized by the Head of Department, when using LPT information systems, all employees are forbidden from participating in Internet discussion groups, chat rooms, or other public electronic forums.
- Participation in discussion groups, chat rooms, and other public Internet forums related to LPT business is restricted to designated employees who have been briefed about the release of confidential or sensitive information.
- Employees shall not advertise, promote, present, or otherwise make statements about LPT's products and services in Internet forums such as mailing lists, news groups, or chat sessions without the prior approval of LPT's Communications Directorate.
- Although the Internet is an informal communication environment, the laws for copyrights, patents, trademarks etc. apply. Employees using LPT systems shall:
 - repost material only after obtaining permission from the source;
 - quote material from other sources only if these other sources are identified;
 - reveal internal information on the Internet only if the information has been officially approved for public release by LPT's Communications Directorate.
- Whenever an Internet user provides an affiliation with LPT --whether implicitly or explicitly, care shall be taken not to make any political advocacy statements or product/service endorsements unless permission of Communications Directorate has first been obtained.
- When using LPT's internet facility, or when conducting LPT business, employees shall not deliberately conceal or misrepresent their identity.
- Electronic mail sent by employees to Internet discussion groups, electronic bulletin boards, or other public forums may be removed if determined to be inconsistent with LPT's business interests or policies.
- Departmental software, documentation, and all other types of internal information shall not be sold or otherwise transferred to any party for any

purpose other than the business purpose expressly authorised by management.

- Exchanges of software and/or data between LPT and any third party must not proceed unless a written agreement has first been signed by GITO.
- Departmental network systems may routinely prevent users from connecting to certain non-business web sites. The ability to connect with a specific web site does not in itself imply that employees are permitted to visit that site.
- No employee nor independent contractor to LPT may use the available Internet, Intranet or E-mail services provided by LPT to access newsgroups, Internet web sites and FTP sites for unauthorised and/or unacceptable purposes such as, but not limited to:
 - the 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 organisation 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 any material supporting any petition, or advertising any services not specifically authorised in writing by the Department;
 - the transmission of any message of an abusive or defamatory nature of anyone either internally or externally;
 - the use of Internet, Intranet or E-mail facilities for any purpose whatsoever not connected to or forming an integral part of Department's operations or business;
 - web sites that advocate any illegal activity.
- All information taken off the Internet must be considered suspect until confirmed by another source.
- News feeds; email mailing lists, push data updates, and other mechanisms for receiving information over the Internet shall be restricted to material which is clearly related to LPT business as well as the duties of the receiving employees.
- Hot-links which transfer a user's Internet session from LPT web site to the web site of any outside entity are not permitted.

- LPT secret, proprietary, or private information shall never be sent over the Internet unless it has first been encrypted by approved methods.
- All software and files down-loaded from non-departmental sources via the Internet (or any other public network) shall be screened with the LPT's approved virus detection software before being run or examined via another program such as a word processing package.
- Users shall not up-load software which has been licensed from a third party, or software which has been developed by LPT, to any computer via the internet unless authorisation from the user's manager has first been obtained.
- All users wishing to establish a connection with LPT's computers via the Internet shall authenticate themselves at a firewall before gaining access to LPT's internal network.
- No systems shall be directly connected to the internet, and employees are prohibited from connecting any servers, desktop computers or laptops to the Internet without the approval from GITO.
- Employees and all users are prohibited from executing Java applets downloaded from the Internet unless the:
 - Applet is from a known and trusted source;
 - Digital signature has been checked and no problem has been discovered.
- Internet access using computers in LPT offices is permissible only via LPT's firewall.
- Other ways to access the Internet, such as direct dial-up connections with an Internet Service Provider (ISP), are prohibited if LPT's computers are employed. Non-departmental computers are prohibited from establishing connection to LPT's networks without specific and prior written permission from GITO.
- Dial out or a connection to any non-departmental systems or networks while simultaneously connected to the LPT internal network is prohibited.
- Testing tools/programs against any Internet system or server is prohibited.
- Dial up connections e.g. whilst traveling or from home based systems and laptop computers which are also utilised for LPT's business must only be made via authorised dial up procedures which employ the use of firewalls.

7.3 PASSWORDS

A computer access password is the primary key to computer security. The importance of password maintenance and security cannot be over emphasized. All employees and users of LPT's computer facilities are solely responsible for the integrity and secrecy surrounding passwords allocated for their usage.

The password uniquely identifies employees and users, and allows access to LPT's information and computer services through logon.

- For your own protection, and for the protection of LPT's resources, everyone must keep his/her password secret and not share it with anyone else.
- Sharing of passwords between users is not allowed.
- All user-chosen passwords for computers and networks must be difficult to guess.
- Passwords shall not be stored in readable form in batch files, automatic login scripts, software macros, terminal function keys, in computers without access control, or in other locations where unauthorised persons might discover or use them.
- All vendor-supplied default passwords shall be changed before any computer or communications system is used.
- All passwords shall be changed immediately if they are suspected of being disclosed, or known to have been disclosed to unauthorised parties
- Regardless of the circumstances, passwords shall never be shared or revealed to anyone else by the authorised user.
- Employees and users are responsible for all activity performed with their personal user-Ids.
- The GITO directorate must automatically activate the principles and characteristics of the user generated password e.g. at least 6 characters in length, alphanumeric etc.
- Screen savers must be activated at least after 10 minutes of inactivity as a maximum, and should be password controlled.
- Boot passwords may be utilised.
- IT Service desk personnel are not permitted to automatically reset or reissue password, and replacement passwords will only be issued once certain prescribed security checks have taken place.

7.4 IT SERVICE/HELP DESK

The IT Service Desk is central to the effective delivery of IT services to LPT and its focus is around monitoring of all user logged requests for service and other related incidents, monitor the resolution process and further provide mechanisms to effectively and timeously resolve them within the agreed service standards.

- To be able to provide the required support, and to ensure that required resources are correctly managed and allocated, all requests for services, problem and incident reports must be routed to the Helpdesk.
- To ensure effective IT service delivery the IT SERVICE DESK and its personnel must be contactable to after office hours to attend to emergency and other ad hoc incidents.

7.5 COMPUTER WORKSTATION USAGE

The LPT has a large variety of information technology related assets which are of great value to LPT's success as a business. These assets include the physical asset and extremely valuable proprietary and confidential information. The loss, theft or misuse of these assets could adversely affect LPT; hence the need to put this policy to regulate the protection of departmental information technology related assets.

- Every employee is responsible to help reduce the possibility and consequences of theft of all personal/LPT computing resources and devices (e.g., desktops, laptops, PDAs and similar hand-held devices), related materials such as diskettes and printed output, and the information they contain.
- All employees regardless of location (e.g. office, car, hotel, plain) where they have the responsibility to appropriately protect the departmental assets.
- All employees are personally responsible for protecting any LPT's property and information entrusted to them and for helping to protect the LPT's asset in general.
- The term Notebook is defined to include any portable computing device including but not limited to notebook computers, laptops, electronic diaries, PDAs, portable scanners etc.
- It is the sole responsibility of the user that his/her notebook is locked to the workstation/desk using a physical cable allocated to them.

- The offices should at all time where OHS&A regulations allows be locked to prevent unauthorized access to the departmental assets and information.
- Employees must at the end of the day lockup all materials (e.g disk, memory stick) that contain departmental information.
- The notebooks must be kept as close as possible to the user/owner, when travelling by air notebooks must not be put in checked baggage.
- Notebooks must not be left for an extended period of time in an unoccupied vehicle. If you must leave your notebook in an unoccupied vehicle, then consider securing the notebook inside the boot of your vehicle.
- Where the provision has been made by the hotel the notebook must be locked in the hotel safe.
- LPT's confidential material recorded on portable media such as paper, diskette, CD, notebook, etc., must be protected according to the same guidelines listed above for protecting your notebook.
- For lost or stolen workstation or LPT's confidential information, the affected party must report the loss or theft to the Risk Management Services and the head of his/her directorate.

7.6 PROTECTION OF DEPARTMENTAL INFORMATION

- All data created, stored or archived on any equipment housed within LPT premises or owned by LPT and used by LPT employees and any other authorized user, is the LPT's property. LPT reserves the right to request and inspect this data at any time without notice.
- The unauthorized possession and/or usage of any equipment or software that could potentially be used to overwrite or alter any of the LPT's data, no matter where or how stored, will result in appropriate disciplinary action being taken.
- A person who without authority intentionally interferes with data in a way which causes such data to be modified, destroyed or otherwise rendered ineffective is guilty of an offence in terms of Section 86(2) of the Electronic Transaction & Communication Act,2002(Act no. 25 of 2002) and may be liable to disciplinary action and/or criminal prosecution.
- Computer workstations available for shared use in any LPT location are not required to have hard disk drive, power-on and keyboard/screen lock passwords applied, and however users must not place LPT's confidential

information, file sharing software, user id files, mail files or databases on such workstations.

- The use of shared data repositories, group websites for storing confidential information or data must be used in accordance with appropriate software security controls and measures to manage the access to the information.
- Security controls must never be set to allow unrestricted access (e.g. “*Everyone*”) to LPT’s confidential information, including your calendar.
- When users store LPT’s confidential information on removable computer media, such as diskettes, tapes, compact disks (CDs), etc., must protect the information against theft and unauthorized access.
- When printing LPT’s confidential information, users must protect the information against theft and unauthorized viewing.
- LPT’s confidential information must only be printed in a controlled access area or attended printer facility.
- When working at non-LPT locations users must ensure that LPT’s confidential information is protected so that it can only be seen or accessed by authorized people
- LPT’s confidential information and material must be locked in a safe environment when not in use - this includes information recorded on portable media such as paper, diskettes, notebooks, laptops, PDAs etc.
- Transmission of LPT’s confidential information to non-LPT’s networks without GITO approval is prohibited.
- It is prohibited to store or process LPT’s confidential information on systems which are not controlled by LPT.
- The printing of departmental information must only be done on printers where the output can be properly protected.
- Employees who participate in confidential teleconferences must confirm that all participants are authorize to participate including listening.
- Storage of confidential information on either intranet or internet servers is prohibited.
- Employees shall not forward information appearing on the Intranet to third parties without going through the appropriate internal channels (such as the HOD or Communications or GITO Directorates).
- Employees are responsible for ensuring that they are utilizing the most up-to-date anti-virus software.

7.7 INTERNAL NETWORKING

- LPT's Intranet and internal LAN systems are for the exclusive use of authorised LPT employees and authorised users.
- The information on the Intranet unlike on internet must be disseminated only to authorised persons.
- The use of network monitoring tool or utilities and network devices that create external connection (e.g. modem, router etc) by users without approval from GITO directorate is prohibited.
- No unauthorised equipment must be connected to any network point within LPT without the prior approval of LPT's GITO.
- The use of peer-to-peer and file sharing software unless authorised to do so is prohibited.
- If you must allow other users to access or store files on your network connected workstation you must select either used access control or password access control when defining the share options for the workstation disk drives and files.
- Users must not allow ANONYMOUS FTP, TFTP, or other unauthenticated access to program or data files on their workstation.
- Before any information is posted to LPT's Intranet, at least two approvals shall be obtained, from LPT's manager in charge of the relevant Intranet page and the owner of the information (or creator of the information if the owner has not yet been designated).
- All content posted to LPT's Intranet remains the property of LPT.
- Employees shall 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 LPT's GITO.

7.8 EXTERNAL NETWORKING

Unlike internal LANs and the Intranet, connections to external public networks and the Internet has the potential to allow any person access to LPT's systems, and it is for this reason that LPT will strictly control the connections to the Internet and other external networks.

- The approval must be requested from GITO directorate to connect to LPT systems and networks from outside LPT premises using remote access services.
- NO unauthorized equipment must be connected to any network point within LPT without the prior approval of department's GITO
- Employees connected via TCP/IP must not be simultaneously connected via a modem to the Internet or any other external TCP/IP network without explicit management authorisation and unless the appropriate TCP/IP commands are entered which prevents intruders from using the workstation as a pathway into the internal network.
- In-house production information systems, such as a server, shall not be directly connected to the internet; instead these systems shall connect with an application server, a database server, or some other intermediate computer that is dedicated to Internet business activity.
- Other ways to access the Internet, such as dial-up connections with an Internet Service Provider (ISP), are prohibited from LPT's owned computers, or any computer connected to any LPT's network or system without authorisation.
- All web servers accessible via the Internet shall be protected by a router or firewall approved by LPT's GITO.
- The establishment of a direct connection between LPT's systems and computers at external organizations (tunnels or virtual private networks) via the Internet or any other public network is prohibited.
- Employees and users shall not make arrangements for, or actually complete the installation of voice or data lines with any carrier, if they have not first obtained approval from the LPT's GITO.
- Information regarding access to LPT's computers and communication systems shall not be posted on the Internet, listed in telephone directories, placed on business cards, or otherwise made available to third parties without the permission of the GITO directorate.
- Users shall not leave modems connected to personal computers in auto-answer mode so that they are able to receive in-coming dial-up calls.

7.9 REQUEST FOR SERVICE

A Request for Service (RFS) is a specific service request that is target date driven. It may also include changes to your PC Hardware, Software and Peripherals, and quotations for the supply of equipment and/or software.

- Users must complete the relevant form and follow applicable procedure to register RFS and forward it to the GITO directorate for necessary processing.
- The average replacement cycle of computer equipment will be four years however it will depend on technology changes and industry standards as well as the availability of financial resources to undertake the replacement.
- NO IT equipment or Software must be purchased, upgraded, installed without the RFS procedure being followed.
- Donated or personal computer equipment must not be utilized in LPT's premises without prior approval from GITO.
- Unless specific permission is obtained, employees will only ever be allowed to have ONE personal computer device allocated to them (e.g. only one PC not a PC and a Laptop).

7.10 NOTEBOOK (LAPTOP) AND OTHER HANDHELD COMPUTERS

Notebook computers and other handheld computing and electronic diary devices are increasingly being utilized by an ever more mobile workforce. Although notebook computers are particularly useful to mobile employees, employees who are issued with notebooks carry extra responsibilities, particularly with regard to data and hardware security.

Notebook computers by their nature and design are portable and easily mislaid, lost or stolen. Apart from the major inconvenience to the employee and the loss of a capital item for LPT, the loss and potential misuse of LPT's information contained on the notebook make it vital that employees issued with notebooks are particularly vigilant.

Employees need to be particularly aware that they are responsible for the physical security of the notebook as well as any data stored on the notebook, hence the need for LPT to control the use thereof.

- Employees who are mobile in terms of job requirement are expected to travel either regionally or internationally, and require computing facilities whilst mobile, may qualify for a notebook.
- The employee must apply to the head of the directorate with motivation as to why he requires a notebook; however the issuing of notebooks will be strictly controlled because of their cost and maintenance requirement and vulnerability.
- Should the notebook be lost, the employee will be held fully responsible for the loss, unless it can be determined that the employee was not at fault.
- Employees are responsible for ensuring that adequate backups of data on the notebook are taken at regular intervals.
- Employees are responsible for the confidentiality of the information on the notebook and need to take due care about where the notebook is used and stored.

7.11 SOFTWARE USAGE & LICENCING

- All software applications developed for use by LPT by 3rd parties becomes the property of LPT.
- All software applications developed for use by LPT's employees becomes the property of LPT.
- Only appropriately licensed software must be installed on LPT's equipment.
- Employees must not "self install" any software (not limited to standard software, games included) without prior GITO's approval.
- Internal Audit and/or GITO will periodically audit LPT's computer equipment.
- Copying and/or distributing software is not allowed.
- Downloading, installing and/or using evaluation, public domain, freeware and shareware is not allowed without prior permission from GITO.
- Any software that is installed (other than centrally controlled standard software) must be appropriately licensed. Employees are required to be able to prove licensing and/or ownership by being in possession of either original purchase order (or valid copy) and/or receipt/packing slip from original vendor and/or documented software license to use and/or original serialized software CD or diskette.
- Software (including all copies if any) purchased by LPT must be returned to LPT upon termination of employment or contract.
- All software licenses certificates and CD must be kept for renewal purpose and reference by the GITO directorate.

7.12 APPLICATIONS

- The GITO directorate has the responsibility to procure or develop all software applications for the various sections (the Customer) on behalf of LPT.
- The user's requirement which include fixing of the problem in an existing system, system enhancement, new system development and purchase of new system from the 3rd party supplier will only be handled by GITO directorate.
- No tender for an IT system may be issued without the approval of the GITO directorate in order to save LPT from expensive duplication of resources, from expensive failures, and to conform to the provisions of the SITA act no 38 of 2002 as amended.

7.13 E-SERVICES WEBSITE

The objective of this section of the policy is to ensure good management and to maintain a high quality of information published on the departmental website.

- All information and service published on the internet must add value to the citizens of Limpopo and South Africa in general.
- The communications directorate reserves the right to decline an application to provide a service or publish information on the website.
- It is the responsibility of the directorate applying to publish information or service on the website to ensure that the content conform to LPT's corporate identity and guidelines and the overall IT infrastructure.
- All requests for the setting up of a facility to publish and maintain information on e-Services Website must follow the normal procedure to request for service.
- It is the responsibilities of the Web Manager to ensure that the requestor is aware of the relevant guidelines related to publication of material on the website and to give necessary assistance.
- Once a service has been added to the e-Services Website, the directorate must take full responsibility to update its content. Each directorate is responsible for the input, correctness, accuracy, timelines, and management of the information it publishes.

- The communication services directorate and the Web Manager will monitor all website content to ensure that content providers maintain the necessary quality of information, and will be responsible for consistency, relevancy and accuracy across the website.

8. POLICY CONTROL

8.1. POLICY AUDIT

Periodic audits will be conducted by GITO directorate, when deemed necessary or as required from time to time, to ensure appropriate application and compliance with this policy.

8.2 POLICY REVIEW

This policy is subject to annual review or when deemed necessary by LPT, to ensure that it is aligned to prevailing legislation and market conditions.

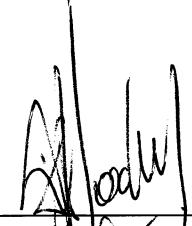
9. EFFECTIVE DATE

This policy will be effective from 22/06/2007 (date)

10. RATIFICATION

This policy was signed on the 22 (day of) JUNE
(month) at POLOKWANE (place)

HEAD OF DEPARTMENT

: 

MEMBER OF EXECUTIVE COUCIL

: 