LIMPOPO

PROVINCIAL GOVERNMENT

REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF

ECONOMIC DEVELOPMENT, ENVIRONMENT & TOURISM

ICT & INFORMATION SECURITY POLICY

2022

Contents

1. ACRONYMS

GB: Gigabyte

GIS: Geographic Information Systems

CGICT: Corporate Governance of Information and Communication Technology

ECT: Electronic Communication and Transactions

HOD: Head of Department

ICT: Information and Communication Technology

IT: Information Technology

LEDET: Limpopo Department of Economic Development, Tourism and Tourism

MEC: Member of Executive Council

PC: Personal Computer

SDI: Spatial Data Infrastructure

SITA: State Information Technology Agency

SMS: Senior Management Services

SCCM: System Center Configuration Manager

2. DEFINITIONS

2.1 **"employees"** mean male and female persons who work for the Department and it Includes interns, and employees/contractors of contracted service providers of any of the corporate entities forming part of LEDET;

2.2 **"exchange server"** is a collaborative enterprise server application that offers electronic mailing, contacts and tasks, calendaring, web-based and mobile information access;

2.3 **"proxy server"** is a computer system or an application that acts as an intermediary for requests from clients seeking resources from other servers, e.g. internet;

2.4 **"map production"** is a process of arranging map elements on a sheet of paper for interpretation; and

2.5 **"meta data"** means Information about the information product such as who captured the data, the manner in which it was collected, date collected etc.

3. INTRODUCTION

This document provides guidelines for the effective management of ICT in LEDET. Information and Communication Technology is a key enabler (tool) in enhancing organisational efficiency in any work environment. Like any other tool, it is necessary to manage and maintain it effectively so that maximum value is derived from it.

As the IT unit, we are tasked with the responsibility of ensuring that the LEDET ICT environment is in sync with the needs of users, while at the same time ensuring that all our IT assets are well maintained and pro-actively managed.

LEDET as an employer is committed to enhancing the efficiency-capacity of its employees by providing qualifying members of staff with the necessary ICT equipment for the performance of their duties. Such equipment is provided on requisition through the normal procurement process and is furthermore subject to procedures as defined by the Supply Chain Management Framework.

ICT in any organisation has the potential to unlock immense value within the organisation and has the ability to positively empower employees to fulfil both their work related and individual goals. Access to ICT, however, carries with it responsibility for both the provider and the user in terms of how it is made available, used and managed.

To this extent, LEDET will endeavour to subscribe to the broad principles of Corporate Governance of ICT as contained in the LEDET CGICT Policy Framework that was instituted by the Department of Public Service and Administration in November 2012; and subsequently adopted by the Limpopo Provincial Administration in 2013.

The policies contained within this package have been developed for the purpose of ensuring that the application of ICT within LEDET is managed in a way that protects the privacy, confidentiality and integrity of information, while at the same time maintaining the physical ICT assets of the Department in good working order.

4. PURPOSE AND OBJECTIVES

4.1 Purpose

The purpose of this policy is to:

4.1.1 establish the basic policy for the Department that will give guidance in the use, procedures, principles, norms, standards, rules and regulations for the protection and preservation of all ICT equipment and information in any form which is generated and owned by and in possession of the Department.

4.2 Objectives

The objectives of this policy are to:

4.2.1 protect the Department's business information and any public information in its custody by safeguarding the confidentiality, integrity, authenticity and availability.

4.2.2 develop principles to protect the Department's information resources from theft, abuse, misuse, distortion and any form of illegal damage.

4.2.3 enforce responsibility and accountability for information security in the Department.

4.2.4 encourage management and staff to maintain an appropriate level of awareness, knowledge and skills which allow them to minimize information risk.

4.2.5 ensure departmental continuity with its activities resulting from unforeseen events.

4.2.6 voluntarily comply with minimum security information requirements as set out in National and Provincial ICT and Information Policy Frameworks.

5. AUTHORITY OF THE POLICY

The policy is issued under the authority of the MEC as the Executive Authority and the HOD as the Accounting Officer for LEDET.

6. LEGAL FRAMEWORK

This policy has been developed within the following applicable legal frameworks:

6.1 The Constitution of the Republic of South Africa Act, 1996 (Act no. 108 of 1996).

6.2 White Paper on the Transformation of the Public Service, 1997.

6.3 Electronic Communication and Transactions Act, 2002 (Act No. 3 25 of 2002).

6.4 Minimum Information Security Standards, 1996.

6.5 Public Service Act, 1994 (Act no. 103 of 1994) as amended.

6.6 Public Service Regulations, 2016.

6.7 Public Finance Management Act, 1999 (Act no. 1 of 1999) as amended.

6.8 Treasury Regulations, 2001.

6.9 Protection of Information Act, 1982 (Act no. 84 of 1982).

6.10 National Information Security Regulations, 1996,

6.11 SITA amendment Act, 2002 (Act no. 38 of 2002).

6.12 Electronic Communications Security Act, 2002 (Act no. 68 2002).

6.13 Public Service IT Policy framework of February 2001.

5.14 Minimum Interoperability Standards (MIOS) for Information Systems in Government, Version 5 of 2011.

6.15 South African Government-Wide Enterprise Architecture Framework (GWEA), 2009.

6.16 Control Objectives for Information and Related Technology 5 (COBIT), 2005.

6.17 International Standards Organization (ISO 9000).

6.18 Information Technology Infrastructure Library, Version 3 (ITIL), 2007.

6.19 South African National Standards, 85300.

6.21 King III Report, 2009,

6.22 Corporate Governance of ICT, 2013,

6.23 POPI Act

7. SCOPE OF APPLICATION

This Policy set applies to all permanent employees LEDET as well as part-time employees, interns, volunteers, contractors, service providers and any other individual/s conducting business with or using LEDET ICT infrastructure.

8. POLICY PRONOUNCEMENTS

This policy is available for access through the LEDET Intranet and all users who have access to the LEDET domain are required to confirm that they have read and understood the provisions of this policy prior to logging-on to the system. http://intranet/publications/policies.html.

As such, all permanent employees, part-time employees, interns, volunteers, contractors, service providers utilising LEDET ICT infrastructure are personally responsible for understanding and following the terms of the policies contained herein, and shall be held personally accountable for the consequences arising from any security violation resulting from a failure to observe such policies. The Department shall identify and provide appropriate information security awareness tools and awareness sessions to support this process.

User Awareness

Personnel are encouraged to familiarize themselves with the policies contained herein. Improved awareness of Information Security 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.

8.1 ICT ACCEPTABLE USAGE POLICY

8.1.1 Purpose

The ICT Acceptable Usage Policy sets out the basic responsibilities of users and system providers with regard to system access and password management issues. This Policy should be read in conjunction with all other LEDET ICT Policies.

8.1.2 System access

(a) The selection of passwords, their use and management as a primary means to control access to systems is to be strictly adhered to according to best practice guidelines.

(b) Users are responsible for all activities done in or from their assigned account.

8.1.3 Lock-out mechanisms

Software lockout mechanisms in case of failed attempted log inns shall be established and enforced.

8.1.4 Passwords

(a) Passwords should include a combination of alphanumeric (upper and lower case) and special characters and should consist of minimum of six characters length.

(b) Passwords must be kept strictly confidential.

(c) Passwords must be changed whenever there is any indication of possible system or password compromise and should be changed every 30 days.

(d) Temporary passwords must be changed at first logon.

(e) Minimum password age 0, Password history 0, Failed login attempts 3, Lockout duration 5, Unlocking of accounts locked by three failed login attempts unlock automatically after 30 minutes

8.1.5 Screen clearing

All users of workstations, PCs or laptops are to ensure that all applications are closed when equipment is left unattended; and systems should be shut-down after hours.

8.1.6 Loading personal screen savers

End users are prohibited from installing screen savers other than the operating system default screensavers.

8.1.7 Securing unattended workstations

All computers must be logged-off when left unattended; and shut-down after hours.

8.1.8 Software updates

All users must ensure that all workstations/notebooks are logged-on to the LEDET domain at least once a week in order to ensure that all necessary software updates are completed.

8.2 ICT BACKUP POLICY

8.2.1 Purpose

The ICT Backup policy sets out the basic responsibilities of users and system providers with regard to data storage and backup procedures. This Policy should be read in conjunction with all other LEDET ICT Policies.

8.2.2 Workstations (All users)

8.2.2.1 Individual computers (Desktop and Notebook Computers)

(a) Important files and data on individual computers must[1] be backed up to the HOME directory on the LEDET File Server on a daily basis.

(b) Each user is assigned 5GB of storage space on the LEDET File Server. This space is assigned only to the designated user and cannot be accessed by any other user.

(c) It is the responsibility of the user to ensure that this storage space is managed and regularly maintained.

(d) Users are responsible for ensuring that all data files and electronic information in their custody whether stored on computers, external hard drives, flash disks and other recordable media are safely stored.

8.2.2.2 Retention periods and disposal of data

(a) Users are responsible for ensuring that electronic data files are archived in accordance with legal and regulatory requirements as stipulated in the LEDET Records Management Policy, file plans and relevant legislative prescripts.

8.2.3 Servers (System Administrators)

8.2.3.1 File Servers

(a) The following files categories must be backed up daily, weekly and monthly on an incremental basis:

- Data stored on home directory
- System State backup

8.2.3.2 Application server

(a) The following files categories must be backed up daily, weekly and monthly on incremental basis:

- System State backup
- Database backup

8.2.3.3 Exchange server

(a) The following files categories must be backed up daily, weekly and monthly on incremental basis:

- System State backup
- Exchange configuration
- Cluster configuration
- User mail boxes

8.2.3.4 Proxy server

The following files categories must be backed up daily, weekly and monthly on incremental basis:

- System State backup
- Proxy Server rule base
- Proxy Server configuration and database backup

8.2.3.5 Software update services

(a) Software must be monitored for updates.

(b) The following updates must be implemented when they are released:

- Windows Software Update Services
- Symantec Live Updates

8.2.3.6 Backup log monitoring

- Backup logs must be monitored weekly.

8.2.3.7 Restore procedure testing

- Data integrity procedure must be activated for all backups.

8.2.3.8 Managing On-Site and Off-Site data stores

(a) Data storage media is filed off-site on a monthly basis.

(b) Off-site and On-site locations where data is stored must provide access controls and protection which reduce the risk of loss or damage.

8.3 ICT E-MAIL POLICY

8.3.1 Purpose

The ICT e-mail policy sets out the basic responsibilities of users and system providers with regard to sending, receiving and management of electronic mail. Emails are now the primary means of business communication.

However, email also presents a significant risk if it is not used responsibly. Users must be cautioned against accepting and opening unsolicited e-mails from sources unknown to them. These e-mails often contain code that is used to gain access to personal information of the user and may be used to commit fraud and other illegal activities. **This Policy should be read in conjunction with all other LEDET ICT Policies.**

8.3.2 Electronic mail (E-mail)

(a) LEDET e-mail should **ONLY** be used for official purposes, using terms and branding which are consistent with other forms of LEDET communication.
(b) Users must refrain from using the "reply to all" response to avoid congestion on the network. Distribution lists should be created to direct emails to relevant recipients.
(c) Users must refrain from sending mass mailings ("send to all").All such mailings must be channelled through Communications Services for consideration and distribution.

8.3.3 Referencing

(a) All official emails should be referenced in accordance with the LEDET File Plans. The reference number must be inserted at the beginning of the subject line.

8.3.4 Legal issues around e-mails

(a) Users are requested to take note that email communications are considered to be legally binding and should therefore be treated as such.
(b) Departmental emails carry a legal-disclaimer and users are cautioned that they may be held individually liable in cases where email is used to misrepresent the Department.

8.3.5 Personal e-mail

(a) The use of departmental email for personal communication is discouraged.
(b) It is recommended that users make use of internet-based email services for private communications.

8.3.6 Receiving electronic mail (e-mail)

(a) Incoming e-mail must be treated with the utmost care due to its inherent information security risks.
(b) E-mail from an unknown source should be deleted.
(c) The opening of file attachments is not permitted unless such attachments have already been scanned for possible viruses or other malicious code.

8.3.7 Retaining or deleting electronic mail

(a) Data retention periods for e-mail should meet legal[3]and business requirements and must be adhered to by all staff.

8.3.8 Receiving misdirected information by e-mail

(a) Unsolicited or 'spam' e-mail is to be treated with caution and be deleted immediately.

8.3.9 Forwarding e-mail

(a) All information forwarded by e-mail (especially attachments) must be correctly addressed and only sent to appropriate persons.

(b) Any security risk (virus, content) associated with the original mail to you will also apply to the forwarded e-mail.

8.3.10 Filtering e-mail content

(a) The organisation will use software filters and other techniques whenever possible to restrict receiving or sending of inappropriate information using email.

8.3.11 E-mail misuse

(a) Mass mailings are strictly prohibited. Notices of acting delegations, events, bereavements, etc. should be forwarded to Communications for upload onto the LEDET intranet.

(b) No private marketing or selling for personal or private gain or for gain of a private company shall be undertaken using the email facility.

(c) Every official shall take extreme to avoid distribution of chain e- mails, which are e-mails that require a recipient to send an email to one or more persons upon a promise of some or other reward, whether direct or indirect, or upon a threat in the event of a failure to forward or transmit such e-mail.

8.4 ICT INTERNET USAGE POLICY

8.4.1 Purpose

The ICT Internet Usage Policy sets out the basic responsibilities of users and system providers with regard to the availability and the accessing, surfing and downloading of content from the internet. This Policy should be read in conjunction with all other LEDET ICT Policies.

8.4.2 Setting up Internet access

(a) The System Administrator must ensure that the LEDET network is safeguarded from malicious external intrusion by deploying a configured firewall.

8.4.3 Access to Internet

(a) Access to the Internet is provided to all users but may be restricted to certain times and/or to certain users should it be deemed fit to do so.
(b) Sites which contain content which is deemed to be inappropriate or offensive or which may pose a security risk may also be blocked.

8.4.4 Downloading files and information from the Internet

(a) Users must exercise care when accessing unknown websites and/or downloading content and files from the Internet to safeguard against malicious code, viruses and inappropriate material.
(b) The accessing of prohibited sites using bypass techniques is not allowed.

8.4.5 Downloaded software

(a) Downloading of unlicensed software is prohibited.
(b) All software on a user's system must be licensed prior to installation.
(c) The downloading of movies, music and other entertainment is prohibited.

8.4.6 Downloaded information

(a) Information on the Internet may be inaccurate, invalid or deliberately misleading, and any decisions based upon it must be considered carefully before use.

8.4.7 Filtering inappropriate material from the Internet

(a) The organisation will use software filters and other techniques whenever possible to restrict access to inappropriate information on the Internet.

8.5 ICT USER ACCOUNT MANAGEMENT POLICY

8.5.1 Purpose

The ICT User Account Management Policy sets out the basic responsibilities of users and network administrators with regard to account management. This Policy should be read in conjunction with all other LEDET ICT Policies.

8.5.2 User registration

All users must complete a domain user account management form to request access to the departmental network and must be approved by the user`s supervisor.

8.5.3 Modifications or changes

The IT Office must be informed by the relevant supervisor in writing of any amendments in the job function, roles and responsibilities of any user where such an amendment may compromise the integrity of the LEDET ICT environment.

8.5.4 User deregistration

(a) Human Resources unit shall be responsible for notifying the IT Office of employees and everyone, such as independent contractors, who will be leaving the Department`s employ or otherwise (through reassignment, extended absence, and so forth) and will no longer need access to ensure that all IT equipment belonging to the Department is retrieved and the access rights of the said user can be terminated.

(b) Upon termination of an employee or other person with access, the IT Office will immediately take the following actions:

- Revoke and disable access privileges, such as usernames and passwords, to systems, data resources and networks.
- Retrieve all hardware, software, data, access control items, and documentation issued to or otherwise in the possession of the user.

- Sixty (60) days after the account is revoked and disabled, the account will be deleted along with all related home directories and mailboxes, unless the directorate has submitted a specific request to IT Office for an extension. Any such request must clearly indicate the specific length of the extension being requested and the final date of account termination that is being requested.

(c) It is the responsibility of the departing employee to delete or transfer all files and email messages that are of a personal nature. These may be transferred to a compact disk or flash storage drive.

8.5.5 Review of user access rights

(a) User access rights should be reviewed by the relevant supervisors and any amendments should be communicated to the IT Office as follows:

- Every six months.
- After any changes such as promotion, demotion or termination of employment.
- When moving from one section or directorate to another.
- Authorisations for special privilege access rights should be reviewed every three months.

8.5.6 Privilege management

(a) The access privileges associated with each system product, e.g. operating system, database management system and each application, as well as the users to which they need to be allocated should be identified.

(b) Privileges should be allocated to users on a need to use basis and on an event by event basis, i.e. the minimum required for their functional role and only when needed.

(c) An authorisation process and a record of all privileges allocated should be maintained by the Network Administrator.

(d) Privileges should not be granted until the authorisation process is complete.

(e) Temporary privileges should be assigned to a different user ID than that used for normal business activities.

8.6 ICT EXTERNAL SERVICE PROVIDERS/CONTRACTORS

8.6.1 Purpose

The policy sets out the basic principles necessary for the secure use and management of LEDET information systems and infrastructure. This Policy should be read in conjunction with all other LEDET ICT Policies.

8.6.2 Access Control

(a) Access to LEDET Information Systems, hardware, software, applications and communications shall be by express permission of the data owner and the IT Directorate.

(b) Contractors must not attempt to enter any LEDET area that houses computer processing or communications equipment unescorted. This applies to data centres, patch rooms, switch rooms and any other rooms housing IT processing equipment.

8.6.3 Acceptable use

(a) All contractors working in a LEDET environment and accessing LEDET Information Systems shall abide by the policies set out in the LEDET ICT and Information Security Policy.

(b) Contractors must adhere to this Policy. Failure to comply with the above policy shall be considered a security breach.

(c) The External Service Providers must ensure that all subcontractors and/or third parties engaged in the fulfilment of its contract with LEDET are aware of and agree in writing to adhere to all provisions contained in this ICT and Information Security policy.

8.6.4 Security Clearance to work in a LEDET facility

(a) Any contractor or service provider working on the system containing sensitive information may be required to obtain the relevant clearance where it is deemed necessary.

8.7 ICT EQUIPMENT POLICY

8.7.1 Purpose

The ICT Equipment Policy sets out the basic responsibilities of users and system providers with regard to the provision, allocation, requisition, procurement, usage and management of ICT equipment. This Policy should be read in conjunction with all other LEDET ICT Policies.

8.7.2 Equipment Allocation

(a) The processing of all requests for ICT equipment is subject to the following:

- The availability of funds
- Adherence to Supply Chain Management guidelines with special emphasis on demand management and asset management
- A written request or motivation from the head of the requesting unit

8.7.3 Desktop Computers

(a) Desktop computers are provided to employees who are, by the nature of their jobs, office bound and who are permanently employed in positions where the performance of their duties will be enhanced by the provision of a personal computer. Such duties will normally fall within the scope of administrative work.

(b) Desktop computers may also be provided as a shared resource for use by employees whose posts do not require them to have full-time access to a computer, but would enable such employees to access email, internet and general word processing functions.

8.7.4 Notebook Computers

(a) Only the MEC, HOD, members of the Executive Management qualify for a notebook computer as a work tool.

(b) Employees who fall outside the categories listed above, but who may require a notebook computer on the basis of specialised work related duties may be provided with a notebook computer provided that the responsible Chief Director provides a detailed motivation outlining the specific functions that require a portable computer approves the request.

(c) Where a notebook computer is required by a non-qualifying employee on a temporary basis, the IT office may, on written request by the relevant Chief Director, make available a notebook computer on loan on a temporary basis as explained in 8.7.10 under Pool equipment.

8.7.5 Printers and other peripheral devices

(a) Standalone desktop printers are issued to the MEC, HOD and SMS Members.

(b) Employees working with confidential information such as Labour Relations officials and Job Evaluation officials may also qualify for a standalone desktop printer, provided that the relevant Chief Director provides a written motivation for the request.

(c) Employees who do not qualify for a standalone desktop printer will be connected to a network printer closest to their office. The ratio of connecting users to a network printer is 10:1. Specialised high-end network printers will be provided for this purpose.

(d) External storage media (excluding External hard Disks drives) are classified as stores items and all requests for these items must be directed to Departmental stores.

(e) Data projectors, plotters, scanners and digital cameras may be issued to sections that require them. A written request with motivation by the relevant Chief Director must be made to the IT Office outlining the need for such a device.

8.7.6 Custodianship of equipment

(a) All ICT equipment remains the property of LEDET.

(b) ICT equipment is allocated to LEDET employees as a tool for fulfilling duties and functions as determined by a particular post.

(c) The employee is personally responsible for the equipment that has been assigned to that post until such time the employee is transferred to another post or another department or resigns.

(d) The Chief Director is the overall custodian of all equipment allocated to his or her Chief Directorate; and should maintain an inventory of all ICT equipment in their respective Chief Directorates.

(e) All employees that have been allocated ICT equipment must take the utmost care in preventing theft, damage or loss of the equipment.

(f) In the unfortunate instance where any equipment has been lost or stolen, the responsible employee must report the matter to the South African Police Services within 24 hours. A case number and a report detailing the incident must then be submitted to the departmental Security and Investigations, Asset Management and the IT Office.

(g) Should any equipment be lost due to the employee's negligence, the employee may be required to pay for the lost item.

(h) No person other than the employee to whom equipment has been allocated may have access to the computer equipment. The exception is the support technicians and the contracted third party hardware maintenance and software support service provider.

(i) Users are encouraged to handle all equipment with care. Mobile equipment should be transported in their appropriate carry bags.

(j) Users are also reminded to ensure that equipment is not left unattended and that offices where equipment resides are kept under lock and key.

(k) Equipment is to be used only for the purpose for which it was issued.

8.7.7 Replacement and renewal of IT equipment

(a) IT equipment will be replaced based on the technical assessment by an IT technician. Only equipment that is beyond repair or is older than 72 months will be considered for replacement.

(b) Equipment retrieved from users will be reallocated to other users. Redundant and irreparable equipment will be disposed of in line with the Supply Chain Management disposal principles.

8.7.8 Requisition of equipment

(a) Equipment requisitions must be made on an official ICT Equipment Request Form by the user and approved by the respective Chief Director.

(b) No verbal or email requests for equipment will be processed.

8.7.9 Transfer of equipment

(a) No employee shall move or transfer equipment from one directorate to another. In cases where such a transfer is required, the equipment should first be returned to the IT office for configuration. Only after Asset Management has done the proper entries in the asset register will the IT Office release the equipment for reallocation or transfer.

(b) An employee who vacates or relinquishes a position by virtue of which she or he had been allocated specific computer equipment must hand over the equipment to his or her supervisor prior to departure.

(c) The supervisor shall accept custodianship of the equipment with effect from the date of vacation or relinquishment by the employee, and return the IT equipment to the IT office within 14 days.

8.7.10 Pool equipment

(a) The Department shall make available pool equipment, where possible to accommodate needs where such needs may not be required on a full-time basis. (e.g. Notebook, Projector, memory device, camera, etc.).

(b) The equipment will be loaned out by the IT office upon written request from the head of the borrowing unit on a first come first served basis.

(c) Pool equipment is a scarce resource and the IT office does not guarantee that equipment will always be available. Loan of pool equipment is limited to a maximum of 14 days, after which reapplication has to be made.

8.7.11 General

(a) An asset allocation form must be completed by the assigned user for each allocated device (attached hereto as annexure 1)

(b) This form shall contain a detailed description, model and serial number of the said device.

(c) The user undertakes not to move, transfer, and re-allocate the device without prior written approval from the IT Office.

(d) Users are strictly prohibited from attempting to conduct repairs or technical modifications on any equipment as this may void any standing warranties or guarantees.

(e) Employees are advised to ensure physical security and care of their assigned equipment.

(f) Special care must be taken in the day to day use of the equipment.

8.7.12 Safe Asset Disposal and Data Privacy

(a) Supply Chain Management Directorate (Asset Disposal Unit) is responsible for the disposal of LEDET absolute asset.

(b) IT Directorate will ensure that all Hard Drives/Media are securely removed, erased/formatted before the assets are disposed.

(c) All employees must ensure that they backup their data before media assets are safely disposed of.

8.8 Antivirus Management and Malicious Software Policy

8.8.1 Purpose

The ICT Antivirus Management and Malicious Software Policy sets out the measures that must be taken by employees to help achieve effective virus detection and prevention. Viruses can be transmitted via e-mail or instant messaging attachments, downloadable internet files, and removable media. Their presence is not always obvious to the computer user. A virus infection can be very costly in terms of lost data, lost staff productivity and / or lost reputation.

This policy applies to all computers that run any operating system and are connected to LEDET network via a standard network connection, wireless access point or virtual private network connection. The definition of computers includes desktop workstations, laptop computers, handheld computing devices and servers.

8.8.2 Roles and responsibilities

8.8.2.1 IT Office

IT is responsible for executing, monitoring and implementing this policy. While safeguarding the network is the responsibility of every user, IT ensures all known and reasonable defences are in place to reduce network vulnerabilities while keeping the network operating.

8. 8. 2.2 User

It is the responsibility of each user to ensure the following:

(a) Devices are regularly connected to the LEDET network to ensure that the latest virus definition (signature) files are installed and/or updated.

(b) The onus is on the user to exercise due care and caution when accessing sites on the internet.

(c) Users must be wary of opening emails from unknown sources, accessing untrusted websites and downloading content which is not work related.

(d) Users must be careful of conducting monetary or banking related transactions with websites that do not have a valid security certificate.

8.8.3 Procedure

(a) Symantec Endpoint Protection anti-virus software is installed on all LEDET desktop workstations and servers running any operating system, following the vendor installation guide provided with the software.

(b) The anti-virus software console window provides complete access to the options available.

(c) The anti-virus software includes the full version of Symantec Endpoint Protection anti-- spyware module, which protects computers from malicious software that is not categorised as a virus. The anti-spyware module blocks spyware, adware, cookies and Trojans.

(d) Real-time Scanning is enabled, and configured so that anti-virus software cannot be disabled on all desktop workstations, laptops, and servers. Real-time Scanning runs automatically and scans a file before opening any file accessed. The Full Scan option is enabled, so that the anti-virus server will conduct scan of all workstations and servers.

(e) The Full Scan item scans every file on each computer, can be memory-intensive, take several hours to complete and it is run when there are known vulnerabilities over night or at the weekend.

To scan a computer hard and flash drive(s) for viruses on an ad- hoc basis, select the Full Scan option in the anti-virus software console window. Antivirus software is configured for live updates to catch new viruses. This is achieved by ensuring that the anti-virus product is updated in terms of both virus definition (signature) files and the scan engine version being used. The antivirus server is configured to check the vendor's website for updates.

(f) All LEDETs servers and workstations are updated from the anti-virus server. If any machine fails an anti-virus update, IT will run a manual update, establish the cause of failure and resolve the issue. Scan engine version patches are only installed onto the anti-virus server when a major version change is implemented. This is done manually from the vendor website, and after being successfully tested, is installed automatically onto all other servers and workstations.

8.8.3 Vulnerability Management

(a) The Department has implemented a "Security Zone" approach to firewall configuration and deployment. These "Security Zones" are implemented as rule-sets on Department firewalls. Default sets of "Security Zones" are created during the implementation of each Department firewall as follows, Workstation Zone, Server Zone and "Demilitarized" Zone.

(b) All computer devices (including servers, desktops, laptops etc.) connected to the LEDET network have proper virus-protection software, current virus-definition libraries, and the most recent operating system and security patches installed.

8.9 Password Management Policy

8.9.1 Purpose

The purpose of this Policy is to present best practice for the creation of strong passwords, the protection of those passwords, and the frequency of change.

8.9.2 Roles and responsibilities

(a) Users must note that passwords are for their own personal use and must not be shared or disclosed to anyone. It is a breach of this policy for any user to misuse their own or other user's password. If any such misuse results in a user knowingly elevating their system privileges above those that they have been authorized to use, that will be considered an act of gross misconduct.

(b) All system-level passwords (e.g. root, enable, Windows admin, application administration accounts, etc.) must be changed at least on a quarterly basis.

(c) Remote access to privileged accounts (e.g. root, enable, Windows admin, application administration accounts, etc.) must not be attempted from insecure locations e.g. open access cluster systems or public terminals.

(d) All user-level passwords (e.g. email, web, desktop computer, etc.) must be changed at least every six months with a recommended change interval of every four months.

(e) A user account that has system-level privileges granted through group memberships or systems such as Dynamic Local User must have a password that is unique from all other accounts held by that user.

(f) Passwords must not be inserted into email messages or other forms of electronic communication.

(g) All user-level and system-level passwords must conform to the guidelines stipulated in 8.9.3.

(h) Change default account passwords

Default accounts are often the source of unauthorized access by a malicious user. When possible, they should be disabled completely. If the account cannot be disabled, the default passwords should be changed immediately upon installation and configuration of the system or application. Implement automated notification of a password change or reset

8.9.3 Guidelines on password selection

(a) All users should be aware of how to select strong passwords. A strong password has the following characteristics:

- It is at least six characters long.
- It includes upper and lower case letters (e.g. a-z, A-Z); digits and other characters, e.g. @ # $ % A & * ( ) – + 1 - - = \ ' {} [1: ll; I < >? I. /)
- It is not a word in any language, slang, dialect, jargon, etc.
- It is not based on personal information, names of family members, etc.

(b) Weak passwords have the following characteristics:

The password:

- contains less than six characters.
- is a word found in a dictionary (English or foreign).
- uses names of family, pets, friends, co-workers, etc.
- uses computer terms and names, commands, hardware, software.
- uses predictable words e.g. 'P@sswOrd', 'Ledet01', 'Administrator01'.
- uses personal information such as addresses and phone numbers.
- uses word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- uses names of any of the above spelt backwards or Preceded/followed by a digit (e.g., secret1, 1secret).

8.9.4 Password protection standards

(a) Same passwords for LEDET domain accounts as for other non- LEDET accounts (e.g. personal account, online banking, e-shopping, etc.).

(b) Where possible, use a different password for different LEDET accounts systems. For example, select one password for your desktop login account and a separate password for your remote access account.

(c) It is prohibited to share LEDET domain accounts passwords with anyone, Including IT staff, administrative assistants or personal assistant.

(d) The 'Remember Password' feature of applications should be avoided. Writing down of passwords on pieces of paper or stored in a file without encryption should be avoided.

(e) In the event that an account or password is suspected to have been compromised, the incident must be reported to IT Office, all passwords are to be immediately changed. IT Office or a delegated official may perform password conformance checks on a periodic or random basis.

8.10 ICT SPATIAL INFORMATION POLICY

8.10.1 Purpose

The ICT Spatial Information Policy sets out the basic responsibilities of users and system providers with regard to GIS. **This Policy should be read in conjunction with all other LEDET ICT Policies.**

8.10.2 Map production

Map products must have the following as minimum:

(a) Departmental branding
(b) Descriptive title
(c) Author
(d) Production date
(e) Source of information depicted
(f) Scale bar
(g) Legend

8.10.3 Archiving of spatial information

(a) Copies of all maps generated must be submitted to the Information Management Chief Directorate in Adobe Portable Format (* pdf) to be made available for internal departmental use via the intranet and to be archived electronically.

(b) Spatial vector and raster electronic data products must be forwarded to Information Management for archiving and distribution to other users. Where the files concerned are still in draft format, this should be clearly indicated both in the metadata and by the inclusion of "draft" in the file name(s).

8.10.4 Metadata

(a) All spatial products must be accompanied by comprehensive metadata which Complies with the provisions of the Spatial Data Infrastructure (SDI) Act of 2003.

(b) Where metadata details (e.g. origin, date, etc.) are not known, this must be clearly indicated

8.11 ICT MAINTENANCE PLAN POLICY

8.11.1 Purpose

The ICT Maintenance Plan Policy sets out routine maintenance activities to be carried out on a regular basis and procedures to be followed in performing this activities. **This Policy should be read in conjunction with all other LEDET ICT Policies.**

8.11.2 Environment

The LEDET ICT environment can be broadly categorised at three levels:

(a) Workstation Level
(b) Server Level
(c) Network Level

8.11.3 Roles and responsibilities

8.11.3.1 System or Network Administrator

(a) Analyse system logs and identify potential issues with computer systems.
(b) Introduce and integrate new technologies into the existing environment.
(c) Perform routine audits of systems and software.
(d) Monitor network traffic.
(e) Perform backups.

(f) Apply operating system and application software updates, patches, and configuration changes.

(g) Install and configure new hardware and software (network and servers).

(h) Responsible for system security.

(i) Troubleshoot any reported problems at network and server level.

(j) System performance tuning.

(k) Ensure that the network infrastructure is up and running.

8.11.3.2 System or Network Controller

(a) Add, remove, or update user account information and resetting passwords.

(b) Attend to all technical queries.

(c) Manage network infrastructure (routers, switches, wireless access points).

(d) Monitor desktop support.

(e) Resolve escalation issues.

(f) Monitor routine maintenance activities at workstation level.

8.11.3.3 Technician

(a) Install and configure new hardware and software at workstation level.

(b) Diagnose and resolve hardware and software issues at workstation level,

(c) Escalate unresolved issues to system controller.

(d) Monitor routine maintenance activities at workstation level.

8.11.3.4 End User

(a) Operate hardware equipment and software applications as per LEDET ICT policies.

(b) Perform routine maintenance operations at workstation level.

(c) Ensure equipment is used responsible and maintained in good condition.

8.12 ICT INCIDENT MANAGEMENT POLICY

8.12.1 Purpose

The ICT Incident Management Policy sets out the procedures to be carried out in the event of failures or errors to prevent recurrence of incidents related to these errors. **This Policy should be read in conjunction with all other LEDET ICT Policies.**

8.12.2 First-level incident management processes

(a) Incident detection and recording (Incident Register)

(b) Classification and initial support

(c) Investigation and diagnosis

(d) Resolution and recovery

(e) Incident closure

8.12.3 Second-level incident management processes

(a) Incident ownership, monitoring, tracking and communication

(b) Establish incident framework management

(c) Evaluation of incident framework management

8.13 PATCH MANAGEMENT POLICY

8.13.1 Purpose

The ICT Patch Management Policy sets out the procedures to be carried out in order to provide a secure network environment for all applications and users. All computer devices (including servers, desktops, laptops etc.) connected to the LEDET network have proper virus-protection software, current virus-definition libraries, and the most recent operating system and security patches installed. **This Policy should be read in conjunction with all other LEDET ICT Policies.**

8.13.2 Roles and responsibilities

8.13.2.1 Information Technology

(a) Responsible for the overall patch management implementation, operations and procedures, while safeguarding the network is the responsibility of every user, IT ensures all known and reasonable defences are in place to reduce network vulnerabilities while keeping the network operating.

(b) To ensure that SCCM is installed and running all the time and that security updates and service packs are automatically deployed to clients computers.

(c) Monitors security mailing lists, review vendor notifications and websites and research specific public websites for the release of new patches. Monitoring will include, but not limited to, the following: Scanning the network to identify known vulnerabilities ,Identifying and communicating identified vulnerabilities appropriate members ,Identifying and communicating identified security breaches to the appropriate members and monitoring Computer Emergency Response Team notifications and websites of all vendors that have hardware or software operating on the LEDET network.

(d) Ensures that SCCM is installed and running all the time. Ensure that security updates and service packs are safe for deployment before are automatically deployed to clients computers.

(e) Monitors security mailing lists, review vendor notifications and websites and research specific public websites for the release of new patches. Monitoring will include, but not limited to the following:

- Scanning the network to identify known vulnerabilities.
- Identifying and communicating identified vulnerabilities to appropriate Members.
- Identifying and communicating identified security breaches to the appropriate members
- Monitoring Computer Emergency Response Team notifications and websites of all vendors that have hardware or software operating on the LEDET network

8.13.2.2 Users

It is the responsibility of each user to ensure that their devices are regularly connected to the LEDET network in order for the latest software updates and anti-virus software to be installed and/or updated.

8.14 ICT SERVICE CONTINUITY POLICY

8.14.1 Purpose

The purpose of this document is to ensure that due consideration is given to the access and availability of transversal ICT systems in the event that the ICT services of LEDET are in any way compromised in the event of a disaster; and to ensure that alternative access mechanisms can be activated within the shortest possible time so that LEDET activities can be resumed normally with minimum citizen discomfort. **This Policy should be read in conjunction with all other LEDET ICT Policies.**

8.14.2 Critical Systems

IT System	Business Process	Business Owner	Operational Responsibility	Infrastructure Requirements
Basic Accounting System	Supplier Payments	Chief Financial Officer	Director: Financial Accounting	Computer with a secure connection to SITA Mainframe and Internet. Access to printer
LOGIS	Capturing of Purchase orders	Chief Financial Officer	Director: SCM	Computer with a secure connection to SITA Mainframe and Internet. Access to printer
	Budgeting	Chief Financial Officer	Director: Budget Management	Computer with a secure connection to SITA Mainframe and Internet. Access to printer
PERSAL	Conditions of Service (Leave	Chief Director Corporate	Director: Human	Computer with a secure connection to SITA Mainframe

	Management Allowances, Terminations)	Services	Resource Management	and Internet. Access to printer
	Salaries (Claims, Deductions, Payroll	Chief Financial Officer	Director : Financial Accounting	Computer with a secure connection to SITA Mainframe and Internet. Access to printer
Electronic mail	Communication	CD: Information Management	Director : Information Technology	Computer with a secure connection to SITA Mainframe and Internet. Access to printer

8.14.3 Service continuity sites

The physical locations and contact points for LEDET ICT service continuity sites are contained in the LEDET ICT DRP and Service Continuity Plan.

8.14.4 Recovery Team

Service	Responsibility
Transversal Systems	SITA
Printing	IT Manager/Network Controller
Desktop	IT Manager/Network Controller
Server	IT Manager/Network Controller
Wide Area Network	IT Manager/Network Controller
Local Area Network	IT Manager/Network Controller

8.15 ICT SERVER ROOM POLICY

8.15.1 Purpose

The ICT Environmental Control Policy provides guidelines for the protection of computer server rooms used to store classified and protected information. **This Policy should be read in conjunction with all other LEDET ICT Policies.**

8.15.2 Access Control

Access to the Server room is controlled by:

(a) Activity monitoring register

(b) Physical door and burglar door

(c) Alarm system

(d) Access Control (ID Cards or Biometric Reader)

8.15.3 Environmental considerations and Climate Control

(a) A fire suppression/protection system will automatically extinguish a fire without the need of human intervention.

(b) Physical and environmental controls specifically smoke detectors and lightning protection must be installed in the building.

(c) The ambient temperature of the server room should be maintained between 18°-27°C with the relative humidity between 40% and 60%.

(d) All the equipment must be raised or in racks at a higher ground level to prevent water damage.

(e) No combustibles (boxes, paper, chemicals, etc.)

(f) No food or other contaminants.

ANNEXURE 1

Sample Asset-allocation form

LIMPOPO DEPARTMENT OF ECONOMIC DEVELOPMENT, ENVIRONMENT AND TOURISM

TRANSFERRING SECTION		**RECEIVING SECTION**	
Directorate/District		Directorate/District	
Building		Building	
Office Number		Office Number	
Location Code		Location Code	
Name of Asset Holder		Name of Asset Holder	
Signature of Asset Holder		Signature of Asset Receiver	
Date		Date	
List of Assets to be transferred			
Description of Item	**Asset No.**	**Serial No.**	**Model**
Period of Loan			
Permanent: Yes	**No**	**Date:**	to

Item received in good working condition		**Yes**		**No**	

Remarks: .....
.....
.....

.....
Signature: Head of transferring Directorate

Date:

.....
Signature: Head of receiving Directorate

Date:

Asset Verification

All assets mentioned in this form were removed from location ....., to location .....
All of them arrived in good condition

Signature: Asset Management Official
Date:

Signature: Office Occupant

Asset Register Update

Processed by: .....

Date: .....

Form No.: ..... of 20.....

ANNEXURE 2

Maintenance Plan Detail

Workstations and Peripherals

No	Actions	Activities	Frequency	Responsibility
1	Operating System Updates	Check and Update: • Security Updates • Patch Management • Service Pack Deployment	 Monthly/Live Monthly/Live Monthly/Live	 Network Administrator/Controller Network Administrator/Controller Network Administrator/Controller
2	Application Software Updates	Check and Update: • Software Versions	Quarterly/Live	User
3	Anti-Virus Updates	Check and Update: • Virus Definitions • Software Versions	Weekly/Live Quarterly/Live	User User/Network Controller
4	Workstation Optimisation	Optimise Hard Disk Space by: • Defragmentation of hard drives • Purging Temporary Internet Files • Flush Deleted Items	 Quarterly Weekly Weekly	 User User User
5	Physical Environment Optimisation	Check and Fix • Cable Connections / Network Points • Dust Accumulation	Quarterly Quarterly	User/Network Controller User/Network Controller
6	File and Data Management	• Backup critical data	Daily	User
7	Reporting	Produce Status Report Of Work Performed And Pending Issues.	Quarterly	Senior Manager: IT

ANNEXURE 3

Servers

No	Actions	Activities	Frequency	Responsibility
1	Operating System Updates	Check and Update: • Security Updates • Patch Management • Service Pack Deployment	 Monthly/Live Monthly/Live Monthly/Live	 Network Administrator Network Administrator Network Administrator
2	Application Software Updates	Check and Update: • Software Versions • Patch Management	 Quarterly/Live Monthly/Live	 Network Administrator Network Administrator
3	Anti-Virus Updates	Check and Update: • Virus Definitions • Software Versions	 Weekly/Live Quarterly/Live	 Network Administrator Network Administrator
4	Server Optimisation	Monitor and Optimise Storage Space by: • Defragmentation of hard drives • Purging Temporary Internet Files • Flush Deleted Items Monitor server event logs and correct errors.	 Monthly Monthly Monthly Weekly	 Network Administrator Network Administrator Network Administrator Network Administrator
5	Physical Environment Optimisation	Monitor and Correct: • Cable Connections / management • Dust Removal	 Quarterly Quarterly	 Network Administrator Network Administrator

No	Actions	Activities	Frequency	Responsibility
		• Environment (temperature) • Fire Safety Measures	Weekly Bi-Annual	Network Administrator Network Administrator
6	File and Data Management	Backup of Data • Monthly (Full) • Weekly (Incremental) • Daily (Incremental)	 Monthly Weekly Daily	 Network Administrator Network Administrator Network Administrator
7	User Account Management	Monitor and Manage User Account Logs	Monthly	Network Administrator/Controller
8	Reporting	Produce Status Report of work performed and pending issues.	Quarterly	Senior Manager: IT

ANNEXURE 4

Network

No.	Actions	Activities	Frequency	Responsibility
1	Maintain Network Infrastructure	Check And Rectify Faults On: • Switches • Routers • Wireless Access Points • Network Printers • Uninterrupted Power Supplies	 Quarterly Quarterly Quarterly Quarterly Quarterly	 Network Administrator Network Administrator Network Administrator Network Administrator Network Administrator
2	Maintain Network Security	• Update Firewall Operating System • Check Firewall Logs • Check Firewall Rules	Quarterly Quarterly Quarterly	Network Administrator Network Administrator Network Administrator
3	Physical Environment Optimisation	Monitor and Correct: • Cable Connections / management • Dust Removal • Environment (temperature) • Fire Safety Measures	 Quarterly Quarterly Quarterly Quarterly	 Network Administrator Network Administrator Network Administrator Network Administrator

ANNEXURE 5

IT Equipment is not a STORES ITEM and are only purchased on request, Please remember there is a process and budget involved in the purchasing of equipment.

You will be notified by email to collect your equipment after it has been delivered and Asset Management has marked the new equipment.

LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
ECONOMIC DEVELOPMENT, ENVIRONMENT & TOURISM

Date :

Chief Directorate :

Directorate :

Location :

User Name : Persal Number : Office no: Contact no:

Intern

Please give a short motivation for your request. Indicate in box, type of request [N] - New, [R] - Replacement, [D] - Damaged or [S] - Stolen.

Important: Where a replacement is required for stolen equipment, please proved SAPS Case no.

Laptop

Desktop

Printer

Scanner

Camera

GPS

Recommended

Name of Senior Manager: Signature: Date:

Approved

Name of General Manager: Signature: Date:

9. DEFAULT

A male or female employee who fails to comply with the provisions of this policy shall be dealt with in terms of the Public Service Disciplinary Code and Procedures for the Public Service.

10. INCEPTION DATE

The inception date of this policy is 30 days after approval by the Head of Department.

11. REVIEW

This policy shall be reviewed every thirty-six (36) months.

12. TERMINATION

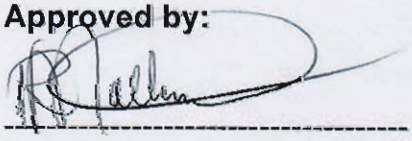
This policy shall remain in force until and unless it has been withdrawn and/or amended.

13. ENQUIRIES

Enquiries regarding the policy shall be directed to the Director: IT Management.

14. APPROVAL

Approved by:



HEAD OF DEPARTMENT

10/02/2022

DATE