LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF

TRANSPORT AND COMMUNITY SAFETY

INFORMATION AND COMMUNICATION TECHNOLOGY (ICT)

SECURITY POLICY

VERSION 1

TABLE OF CONTENTS

PAGES

1. Acronyms and abbreviations

1. DNA: District Network Administrator
2. DTCS: Department of Transport and Community Safety
3. Firewall: A device designed to permit or deny network transmissions based upon a set of rules and is frequently used to protect networks
4. GITO: Government Information Technology Office(r)
5. HoD: Head of Department
6. ICT: Information and Communication Technologies which is a "diverse set of technological tools and resources used to communicate, and to create, disseminate, store, and manage information." These technologies include computers, the Internet, broadcasting technologies (radio and television), and telephony.
7. IT: Information Technology which is concerned with the development, management, and use of computer-based information systems.
8. MBSA: Microsoft Baseline Security Analyzer.
9. NTFS: New Technology File System which is the standard file system of windows.
10. OS: Operating System which is a collection of software that manages computer hardware resources and provides common services for computer programs.
11. SITA: State Information Technology Agency.
12. UPS: Uninterruptable Power Supply.
13. VPN: Virtual Private Network
14. WSUS: Window Server Update Services which is a computer program developed by Microsoft Corporation that enables administrators to manage the distribution of updates and hotfixes released for Microsoft products to computers in a corporate environment.

2. EXECUTIVE SUMMARY

While the use of Information Technology is crucial to boost overall productivity and improving service delivery to the public, DTCS can/may incur unnecessary threats and be subject to risk(s) of losing crucial information. The aim of this policy is to ensure that the Department influences the investment in its IT Security. Recognizing that IT Security shall reasonably require a portion of departmental budget.

To ensure that critical business activities take place and prevent loss of data, unauthorized access or hacking of the network, IT Security should be implemented to prevent various security threats and environmental hazards. This policy has been developed to ensure that the IT infrastructure is protected and officials understand the importance of IT security starting from logging on to the computer until any system allocated to the user.

INTRODUCTION

This policy applies to all employees, contractors, and other authorized third party entities that use the Limpopo Department of Transport and Community Safety's computer network. In order to safeguard the Department's information technology resources and to protect the confidentiality of data, adequate security measures must be taken.

This Information Technology Security Policy (hereafter, "IT Security Policy") reflects the Department's commitment to comply with best practice principles that govern, protect, and secure sensitive and confidential information, as well as ICT equipment. Wherever possible, this policy attempts to establish a balance between the risk of loss of information resources, including data misuse, and the effort and cost of the security measures. It includes provisions to reduce, as far as feasible, the risk of theft, fraud, destruction or other misuses of the Department's IT resources.

Administrative information processing, digital telecommunications and related technology are critical business operations of the Department. Inappropriate exposure of confidential and/or sensitive information, loss of data and inappropriate use of computer networks and systems can be minimized by complying with reasonable standards, attending to the proper design and control of information systems and applying sanctions when violations of this Security Policy occur.

Security is the responsibility of everyone who uses the Department's Information Technology resources. Every employee, contractor and authorized 3rd party entity should become familiar with this Policy's provisions and the importance of adhering to it when using the Department's computers, networks, data and other information resources. Each is responsible for reporting any suspected breaches of its terms to GITO. The Department's computers and computer workstations, terminals, network printers and other devices either owned by the Department or authorized by the Department to connect to its networks are primarily for Departmental business functions. IT equipments are property of the state including all the information

contained in them. The department through office of GITO has a right to access computers to ensure compliance with set policies and/or during investigation periods without a user's consent.

3. PURPOSE AND OBJECTIVE OF THE POLICY

The purpose of the policy is to establish rules to insure the protection of confidential and/or sensitive information stored or transmitted electronically and to ensure protection of the Department's information technology resources. The policy assigns responsibility and provides guidelines to protect the Department's systems and data against misuse and/or loss.

4. AUTHORITY OF POLICY

The authority of this policy lies within the Office of Executive Authority for the Department.

5. LEGAL FRAMEWORK

Any third party who has a contractual relation with the Department and contravenes the provision of the policy will be dealt with in terms of the penalty clause of the agreement entered into by and between him/her and the Department.

Employees who violate this policy will be disciplined in terms of measures contained in or published in one or more of the following acts, regulations and policy prescripts (this list is by no means exhaustive):

3.1 Disciplinary Codes and Conducts
3.2 Public Service Act, 1999
3.3 Public Service Regulations 2001 as amended
3.4 Public Finance Management Act, 1999 (Act No.1 of 1999)
3.5 Treasury Regulations issued in terms of PFMA, 1999
3.6 State Information Technology Act (Act no 88 of 1998)
3.7 Protection of Information Act (Act no 84 of 1982)
3.8 Minimum Information Security Standards (MISS), Second Edition March 1998

3.9 Any other applicable legislature and ICT policies of the Department

6. SCOPE OF APPLICATION

This policy applies to every computer and computer workstation, terminal, network printer and other device either owned by the Department or authorized by the Department to connect to its networks. It also applies to every employee, contractor, intern, learner and authorized 3rd party entity accessing the Department's networks and resources.

7. DEFINITIONS

i. Accountability: Ensuring that the actions of an entity/individual may be traced uniquely to that entity/individual, who may then be held responsible for that action

ii. ASCII: American Standard Code for Information interchange. It is the character–encoding scheme based on the ordering of the English alphabet. ASCII codes represent text in computers, communications equipment, and other devices that use text.

iii. Authentication: Establishing the validity of a claimed entity/verification of the identity of an individual or application

iv. Availability: Being accessible and useable upon demand by an authorised entity

v. Confidentiality: The principle that information is not made available or disclosed to unauthorised individuals, entities or processes

vi. Cryptographic devices: Devices to encrypt and decrypt electronic data
Identification and Authentication: Functions to establish and verify the validity of the claimed identity of a user

vii. Information Technology: Any equipment or interconnected system or subsystem of equipment, that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of vocal, pictorial, textual and numerical data or information

viii. Integrity: the inherent quality of protection that maintains the accuracy of entities of an information and communication system and ensures that the entities are not altered or destroyed in an unauthorised manner

ix. Monitoring: Performance measurement to ensure the confidentiality, availability and integrity of operational systems and information

x. Network Devices: Computers and devices interconnected by communications channels that facilitate communications among users.

xi. Password: Confidential authentication information composed of a string of characters

xii. Patch: A piece of software designed to fix problems with or update a computer program or its supporting data.

xiii. RAS DIAL-BACK: Method of using a telephone line to dial into the network

xiv. Remote access: The access of remote users to corporate IT services by means of telephone lines or 3G data card through a gateway/computing that is performed at a location that is distant from a central site, over a network connection

xv. The Department: Limpopo Department of Transport.

xvi. Vendor: A supplier who provides goods or services to a company.

8. POLICY PRONOUNCEMENT

Implementation of this policy will be guided by Batho Pele Principles and any other piece of relevant legislation.

9.1. ROLES AND RESPONSIBILITIES

i. GITO is responsible for ensuring that information resources are maintained in compliance with the Department's IT Security policies and procedures.

ii. Administrators of systems that are not managed by GITO are responsible for ensuring that their systems are maintained in compliance with the Department's IT Security policies and procedures.

iii. The IT Security Manager is responsible for auditing and monitoring information Systems to ensure that they comply with the IT Security Policy of the Department.

iv. The DNA's and Head Office Technicians are responsible to make sure that they are keeping systems in compliance with the IT Security Policy of the Department.

v. Human Resources Management Directorate will be responsible for informing IT regarding staff movements, i.e. transfer of staff in and out of the Department, new appointment, death, termination of employment or voluntary retirement and resignation. This information is to be supplied to IT a month in advance where appropriate.

9.2. CONTROLLED ACCESS

i. An employee of the Department shall be granted access to only the classified level of information and assets for which appropriate access authorization(s) and the need to know have been approved.

ii. A person shall be granted access to only those IT system resources necessary to perform the assigned functions and only when such access will not lead to a breach of this or any other security principles.

iii. Appropriate segregation of duties, specifically allocated and defined in writing, shall apply.

iv. Controlled access will be achieved via physical and procedural means. Unique identification of the user to the system must be provided. An access authorisation structure shall determine access and privileges, grant such access and privileges and record, control and monitor these.

v. A formal procedure to get a user account is as follows:

- A user creation form shall be issued to the requester to complete; See annexure A.
- Systems to be accessed should be clearly listed on the request form;
- A form shall be signed by the requester, immediate supervisor, IT Technician and a GITO/Director IT;
- Domain user accounts shall be created upon approval. The structure of the user account shall be formulated using a surname and first initial of the user;
- The computer name of all desktops and laptops shall contain the exact username of the user.

9.3. DATA BACKUP

i. A full backup must be performed by responsible IT official at least once per month. IT security manager/official to audit the backups once per month.

ii. Daily backups must be performed as incremental backups.

iii. Backups must be scheduled to run automatically every night.

iv. Backup logs must be checked on a daily basis to ensure successful completion of backups.

v. Completed backups must be stored off-site according to the SITA service level agreement.

vi. All tapes and backups must be validated and tested at least once every three months. Test results will be kept and filed for record purposes.

vii. Tapes should be clearly labeled and used in strict rotation (according to the rotation schedule) to ensure even wear.

viii. Tapes must be replaced at the first sign of deterioration and according to the manufacturer's recommendations.

9. PHYSICAL SECURITY

10.1. All server and switch rooms must be constructed with concrete walls, raised floors and fire resistant doors.

10.2. All third-party vendor access to server and switch room must be logged in a register in format (Name, Surname, ID No, Company, Date and Time).

10.3. Third-party vendors must be accompanied by a GITO staff member at all times.

10.4. This exclude the Server Administrator provided by SITA as per SLA.

10.5. Where possible, server and switch rooms should be equipped with a temperature monitoring system which allows for alerts to be sent by e-mail and sms when a high or low temperature alarm is triggered.

10.6. Log files must exist for equipment maintenance schedules according to manufacturer's specifications.

10.7. All computer equipment in server and switch rooms must be connected to a UPS device.

10.8. The UPS must be tested annually and batteries checked for recommended use dates and physical defects.

10.9. Where possible UPS's should be equipped with monitoring system which allows the backup generator fuel levels should be checked on a weekly basis.

10.10. The backup generator should be tested on an annual basis.

10.11. The backup generator should be serviced according to manufacturer's specifications and a log should be kept.

10.12. A fire detection system should be present in every server and switch room.

10.13. Where possible a fire preventions system (Halon or CO2) should be present in server and switch rooms.

10.14. Before temporary off site removal of any computer equipment, a computer removal document must be filled in and approved.

10.15. Server rooms must be equipped with electronic access control devices and logs kept of all entries.

10.16. Switch rooms must be locked when access is not required.

10.17. A print out of access control logs to the server room is required on a monthly basis.

10.18. All unused computer equipment must be stored in a secure location.

10.19. Users are responsible for the safe keeping of equipment assigned to them.

10. USER ACCOUNT AND PASSWORD MANAGEMENT

11.1. All accounts shall be reviewed at least quarterly to ensure that access and account privileges are commensurate with job function, need-to-know, and employment status.

11.2. The Human Resource Management Directorate will ensure that GITO be informed at least one month in advance of any new appointments. No user account will be created or modified without a signed New/Modified User Form.

11.3. All user accounts will be disabled immediately by the Network Administrator, upon an employee's departure from the Department either by dismissal, transfer, resignation, retirement, death or any other forms of departure. The Network Administrator will produce a monthly report for the Deputy Director GITO, providing details regarding the disabled user accounts. The disabled account to be permanently deleted after 12 months of departure.

11.4. An employee's access to a user account will be changed/modified by the Network Administrator, once the employee has transferred to a different directorate; in accordance with the employee's new job functions and requirements.

11.5. The Human Resource Management Directorate will ensure that GITO are informed at least one month in advance of any resignations or transfers. This must be done by signing a User Termination Form.

11.6. All user accounts at the Department are created as Standard User Accounts. This means that users have standard privileges to log onto the network, use network printers that have been assigned to them, access their email, and use the internet and any other privilege that is a core requirement of their job function (i.e. BAS, PERSAL and LOGIS). BAS users will be given local administrative rights.

11.7. User names are standardized and the employee's PERSAL number is used to enable the user to log onto the network, and user's computer. Email addresses are also standardized with the employee's surname and first initial. In the instance where there are users with same surname and initial, the user's full name may be used as an email address. The password that an employee uses to log onto the network will be applied to access the employees email account and internet application.

11.8. Users that work on transversal systems (i.e. BAS, LOGIS and PERSAL) will be issued with system passwords in order to access the applications. The system passwords are only issued by the relevant System Controllers and not the GITO of the Department. This policy can be read with Financial Management User and Account Management Procedure manual.

11.9. Internship Programme personnel and temporary appointed contractors will be issued with usernames and passwords, which will be operative until their services are terminated.

11.10. All users shall complete a *User Creation Form* prior to them being created on the domain and standard system. The form must be signed by the new user and be signed by the supervisor to endorse the request. See Annexure A.

11.11. User Account lockout must meet the following conditions:

a. Lock Out duration: (To be unlocked by IT officials)
b. Lock out threshold: (3 invalid logon attempts)
c. Reset account lock out counter after: (To be unlocked by IT officials)

11.12. Passwords must not contain the user's entire Account Name value, month, Password or Full Name value. Both checks are not case sensitive.

11.13. Passwords complexity must contain characters from three of the following five categories:

a. Uppercase characters of European languages (A through Z, with diacritic marks, Greek and Cyrillic characters)
b. Lowercase characters of European languages (a through z, sharps, with diacritic marks, Greek and Cyrillic characters)
c. Base 10 digits (0 through 9)
d. Any Unicode character that is categorized as an alphabetic character but is not uppercase or lowercase. This includes Unicode characters from Asian languages.
e. Non alphanumeric characters: ~!@#$%^&* _-+=`|\(){}[]:;'"<>,.?/

11.14. Password must meet complexity requirements.

11.15. Passwords must never be written down on a piece of paper.

11.16. Password length must be a minimum of seven (7) characters.

11.17. Password history (must not repeat last 10 passwords used).

11.18. Never share passwords with anyone.

11.19. Use different passwords for all user accounts.

11.20. Passwords should be changed every 30 days.

11.21. Requests for password change by users will be processed after *Password Change Request Form* has been completed. The form must be signed by both the requester and the technician handling the request. See Annexure B.

11. VIRUS PROTECTION

12.1. Every system must be protected by anti-virus software.

12.2. Configurations must allow for removable media to be scanned before allowing access on the Departments network.

12.3. A scheduled scan must be conducted on a monthly basis.

12.4. Automatic updating must be configured to allow for the latest virus definitions in order to keep systems secure and protected against latest threats.

12.5. Reporting must be enabled in order to monitor and manage threats.

12.6. Anti-Virus clients must be configured to prevent users from disabling anti-virus protection.

12.7. Anti-Virus software version will be updated annually.

12.8. Systems not on the network must be updated manually on a monthly basis.

13. FIREWALLS

13.1. All external connections must be protected by a firewall.

13.2. Every firewall must be configured with a deny-by-default policy.

13.3. Internet Access must be controlled by a proxy server/Vodacom line.

13.4. Authentication to the firewall must be controlled by individual account access and the administrator user name and password must be changed and renamed.

13.5. User accounts must be assigned with the lowest level of privileges required to perform duties.

13.6. Firewall firmware version software should be patched and updated on a regular basis.

13.7. Logging of firewall data should be enabled.

13.8. Logs should be reviewed on a weekly basis.

13.9. Logs should be archived on a monthly basis.

13.10. Configuration logs should be backed up on a monthly basis and after every configuration change.

13.11. Administrators should be alerted in the event of possible attacks and in the event of system failure.

13.12. Control measures shall be put in place for all the ports that need to be opened on all the firewall. Request for opening ports on the firewall shall require a formal detailed request from the Deputy Director of Network Infrastructure, with the timeframe those ports need to be opened and the request need to be recommended by an Director: Information technology and approved by the Chief Director: GITO. The form is annexed as C.

14. REMOTE ACCESS CONNECTIONS

14.1. Remote access connections are not allowed unless when it is necessary to do so and request has been sent to GITO for analysis and approval.

15. WORKSTATION SECURITY

15.1. The "auto run" function for removable devices and CD-ROMs must be disabled.

15.2. A standard image must be configured for every model number of workstation.

15.3. The standard image must include anti-virus, latest patches, drivers and software.

15.4. The standard image must be reviewed on a monthly basis.

15.5. Users are not allowed to have administrative access on workstations and Laptops unless they are BAS or any system users that need to install .exe file.

15.6. Local administrator accounts must be renamed.

15.7. User "My Documents" and "Desktop" folder must be redirected to a server shared drive to enable backups to be performed.

15.8. Automatic updates must be configured to obtain the latest patched from the SCCM server.

15.9. In cases where client data contains sensitive information, encryption software must be used to protect the data.

15.10. Security and event logs must be available for a minimum of 30 days.

15.11. Any services that are not needed must be disabled.

15.12. A screensaver password must be configured.

16. SERVER SECURITY

16.1. All new servers must be deployed by using a standard image or manual configuration.

16.2. The standard image must include anti-virus, latest patches, drivers and software.

16.3. The standard image must be reviewed before implementing on any newly procured server.

16.4. All users with administrative access must be documented.

16.5. The local and domain admin accounts must be renamed and passwords changed.

16.6. Automatic updates must be configured to obtain the latest patched from the SCCM server.

16.7. All volumes should be formatted with the NTFS file system.

16.8. All events must be logged and log files exported and archived.

16.9. Log files should be reviewed on a weekly basis before archiving.

16.10. All services that are not needed must be disabled.

16.11. All servers must be secured with the MBSA tool on a regular basis.

16.12. A screensaver password must be configured.

17. CLIENT DATA

User Data folders must have permissions enabled and only the owner of the folder and files and administrators should be allowed access to these folders.

18. UTILISATION OF PRIVATE COMPUTERS

When private computers are used, written approval shall be obtained from GITO to use a private computer for official purpose. A computer register shall be established containing full personal particulars of the person, as well as details of the computer. Classified information bearing a sensitivity of Confidential or higher shall not be stored on a private computer.

19. DISASTER RECOVERY

An approved disaster recovery plan and procedures should exist to minimize the impact of any type of disaster on the IT Systems. It should be classified as Top Secret and handled on a need-to-know basis.

20. MOBILE DEVICES - MODEMS AND DIAL-UP COMMUNICATIONS

No modems shall be connected to communication networks without the authorization from GITO. Authorization shall only be given on receipt of a detailed motivation approved by the particular employee's Director, requesting such facilities and a security plan detailing the manner in which the use of the modem and classified information transmitted through this modem will be regulated and controlled. The use of such equipment on the ICT infrastructure of the Department is subject to approval by the HoD.

Other mobile devices like I-Pads and mobile smart phones shall be allowed to connect to the Department's email facility for sending and receiving of emails. These mobile devices shall be correctly configured to access the Departmental email facilities as per the device operational manual. Users shall familiarize themselves with the operation of these devices and the security risks involved.

21. MONITORING AND EVALUATION

GITO will monitor the implementation of this policy. Monitoring and Evaluation Unit within the Department will also track progress and policy achievement in terms of the objectives.

22. DEFAULT

This policy is the Departmental guide of GITO and anyone who violates the provision of this policy will be dealt with in terms of this policy or any other contractual clause between the Department and the accused.

23. INCEPTION DATE

This policy comes into effect from the 1st day of the next month after date of approval.

24. TERMINATION AND REVIEW OF THE POLICY

The policy and its annexure(s) shall be reviewed every 36 months or when need arise.

25. ENQUIRIES

Enquiries regarding this policy should in the first instance be directed to the GITO.

RECOMMENDED / NOT RECOMMENDED

ACCOUNTING OFFICER — **DATE** 19/3/21

APPROVED / NOT APPROVED

MEMBER OF EXECUTIVE COUNCIL — **DATE** 30/03/2021