LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

DEPARTMENT OF
ROADS AND TRANSPORT

INFORMATION TECHNOLOGY SECURITY POLICY

VERSION 2

TABLE OF CONTENT

ACRONYMS AND ABBREVIATIONS

1. 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.
2. DNA - District Network Administrator.
3. GITO - Government Information Technology Office.
4. MBSA refers to Microsoft Baseline Security Analyzer.
5. NTFS - New Technology File System which is the standard file system of windows
6. OS - Operating System which is a collection of software that manages computer hardware resources and provides common services for computer programs.
7. SITA - State Information Technology Agency
8. UPS - Uninterruptable Power Supply.
9. 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.
10. 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.
11. IT - Information Technology which is concerned with the development, management, and use of computer-based information systems.

DEFINITIONS

1. Firewall - a device designed to permit or deny network transmissions based upon a set of rules and is frequently used to protect networks
2. Network Devices - computers and devices interconnected by communications channels that facilitate communications among users.
3. Patch - a piece of software designed to fix problems with or update a computer program or its supporting data.
4. The Department - Limpopo Department of Roads and Transport.
5. Vendor - to a supplier who provides goods or services to a company.

1. INTRODUCTION AND BACKGROUND

This policy applies to all employees, contractors, and other authorized third party entities that use the Department'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.

2. PURPOSE AND OBJECTIVE

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.

3. USER AWARENESS

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 the IT Manager Security.

The Department's computers and computer workstations, terminals, telephones, facsimile machines and other devices either owned by the Department or authorized by the Department to connect to its networks are primarily for Departmental business functions. As such, all information technology resource users within the Department are expected to:

a. Respect the privacy of other users.
b. Respect the rights of other users.
c. Respect the intended use of resources and systems.
d. Respect the integrity of the system or network.
e. Adhere to all Departmental policies and procedures mandated by the GITO.

4. DOCUMENTS THAT SHOULD BE READ WITH THE POLICY

Patch Management Procedures document.

5. SCOPE OF APPLICATION

This policy applies to every computer and computer workstation, terminal, telephone, facsimile machine and other devices either owned by the Department or authorized by the Department to connect to its networks. It also applies to every employee, contractor and authorized third party entity accessing the Department's networks and resources.

6. ROLES AND RESPONSIBILITIES

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

6.2 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.

6.3 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.

6.4 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.

6.5 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.

7. LEGAL FRAMEWORK

7.1 Disciplinary Codes and Conducts

7.2 The Provincial Policy Development Framework (2012)

7.3 Departmental Policy Development Framework Version 2 (2012)

7.4 Public Service Act, 1999

7.5 Public Service Regulations 2001 as amended

7.6 Public Finance Management Act, 1999 (Act No.1 of 1999)

7.7 Treasury Regulations issued in terms of PFMA, 1999

7.8 Any other applicable legislation, regulation or policy

8. POLICY PRONOUNCEMENT

Implementation of this policy will be guided by Batho Pele Principles.

9. IT SECURITY

9.1 Data Backup

9.1.1 A full backup must be performed by the IT security officer at least once per month.

9.1.2 Daily backups must be performed as incremental backups.

9.1.3 Backups must be scheduled to run automatically every night.

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

9.1.5 Cleaning of backup devices should be performed according to manufacturer's specifications.

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

9.1.7 All tapes and backups must be validated and tested at least once every three months.

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

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

9.2 Physical Security

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

9.2.2 All third-party vendor access to server and switch room must be logged in a register in the format (Name, Surname, Company, Date and Time).

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

9.2.4 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.

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

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

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

9.2.8 Where possible UPS's should be equipped with monitoring system which allows for alerts to be sent by e-mail and sms during power failures and low battery alarms.

9.2.9 The backup generator fuel levels should be checked on a weekly basis.

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

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

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

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

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

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

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

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

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

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

9.3 User Account and Password Management

9.3.1 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.

9.3.2 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.

9.3.3 All user accounts will be terminated 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 GITO, providing details regarding the terminated user accounts.

9.3.4 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.

9.3.5 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.

9.3.5 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 FINEST).

9.3.7 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.

9.3.8 Users that work on transversal systems (i.e. BAS, FINEST 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.

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

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

9.3.11 Passwords 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: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/

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

9.3.13 Never share passwords with anyone.

9.3.14 Use different passwords for all user accounts.

9.3.15 Passwords should be changed every 30 days.

9.4 Virus Protection

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

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

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

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

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

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

9.5 Firewalls

9.5.1 All external connections must be protected by a firewall.

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

9.5.3 Internet Access must be controlled by a proxy server.

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

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

9.5.6 Firewall software should be patched and updated on a regular basis.

9.5.7 Logging of firewall data should be enabled.

9.5.8 Logs should be reviewed on a weekly basis.

9.5.9 Logs should be archived on a monthly basis.

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

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

9.6 Patch Management

9.6.1 Automated tools will scan for available patches and patch levels, which will be reviewed as specified in the Patch Management Procedures document.

9.6.2 Manual scans and reviews will be conducted on systems for which automated tools are not available.

9.6.3 Vendor supplied patch documentation will be reviewed in order to assure compatibility with all system components prior to being applied.

9.6.4 Where possible, patches will be successfully tested on non-production systems installed with the majority of critical applications/services prior to being loaded on production systems.

9.6.5 Successful backups of mission critical systems will be verified prior to installation of patches and a mechanism for reverting to the patch levels in effect prior to patching will be identified.

9.6.6 Patches will be applied during an authorized maintenance window in case where the patch application will cause a service interruption for mission critical systems.

9.6.7 Patches will be prioritized and applied in accordance with the Patch Management Procedures document.

9.6.8 Logs will be maintained for all system categories (servers, secure desktops, ASCII, switches, etc.) indicating which devices have been patched. System logs help record the status of systems and provide continuity among administrators. The log may be in paper or electronic form. Information to be recorded will include but is not limited to date of action, administrator's name, patches and patch numbers that were installed, problems encountered, and system administrator's remarks.

9.6.9 In the event that a system must be reloaded, all relevant data on the current OS and patch level will be recorded. The system should be brought back to the patch levels that were in effect before reloading started.

9.7 Remote Access Connections

9.7.1 Remote access connections are not allowed.

9.8 Workstation Security

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

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

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

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

9.8.5 Users are not allowed to have administrative access on workstations and Laptops.

9.8.6 Local administrator accounts must be renamed.

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

9.8.8 Automatic updates must be configured to obtain the latest patched from the WSUS server.

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

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

9.8.11 Any services that are not needed must be disabled.

9.8.12 A screensaver password must be configured.

9.9 Server Security

9.9.1 All new servers must be deployed by using a standard image.

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

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

9.9.4 All users with administrative access must be documented.

9.9.5 The local and domain admin accounts must be renamed and passwords changed. Automatic updates must be configured to obtain the latest patched from the WSUS server.

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

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

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

9.9.9 All unneeded services must be disabled.

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

9.9.11 A screensaver password must be configured.

9.10 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.

10. REVIEW AND TERMINATION OF THE POLICY

The policy will be reviewed every 24 months based on the comments and inputs from the stakeholders and it will be terminated upon the inception of the new policy.

11. 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.

12. DEFAULT

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 prescripts that are contained in the Legal Framework of this policy.

13. INCEPTION DATE

The inception date of this policy will be within 30 days after the approval by the Authority

14. ENQUIRIES

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

RECOMMENDED / ~~NOT RECOMMENDED~~

_____

_____

_____

_____ 14/12/2012

ACCOUNTING OFFICER **DATE**

APPROVED/~~NOT APPROVED~~

_____

_____

_____

_____ 25/01/2013

MEMBER OF EXECUTIVE COUNCIL **DATE**