



LIMPOPO
PROVINCIAL GOVERNMENT
REPUBLIC OF SOUTH AFRICA

**DEPARTMENT OF
ROADS AND TRANSPORT**

PASSWORD POLICY

1. Introduction

- 1.1 Passwords are an important aspect of Information and Communications Technology (ICT) and computer security. They are the front line protection for a user's computer system. A poorly chosen or weak password may result in the compromise of a user's computer system, private confidential information or the department's network. The task of the Government Information Technology Office (GITO) is to ensure that all users on the network have secure passwords that provide integrity and confidence to a user's information system.

2. Purpose of the Policy

- 2.1 The primary purpose of this policy is to create awareness and emphasize the importance of such a policy to users. The policy also serves as a guideline for users to create strong passwords, protection of an employee's password and the frequency of change of employee's password.

3. User Accounts

3.1 Standard User Accounts

- 3.1.1 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 (BAS, PERSAL and FINEST).
- 3.1.2 User names are standardized and the employee's PERSAL number is used to enable the user to log onto the network, and users computer. Email addresses are also standardized with the employee's surname and first initial. In the instance where there are users with same the 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.
- 3.1.3 Users that work on transversal systems (BAS, FINEST and PERSAL) will be issued with system passwords in order to access the application. The system passwords are only issued by the relevant System Controllers and not the GITO.
- 3.1.4 In-service students and temporary appointed contractors will be issued with usernames and passwords, which will be operative until their service is terminated.

3.2 Administrator Account

- 3.2.1 Administrator Account access is given to all Network Administrators, the IT Manager and the Systems Manager within the GITO. The Administrator Account has full privileges on the network that enables the Administrators to perform all network tasks, additions, configurations and changes. The account also permits the Administrator to have access to all the users' computers and files for **support and administration purposes only**.

4. Termination or Change of User Accounts (Access Rights)

- 4.1 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.
- 4.2 An employee's access to a user account will be changed by the Network Administrator, once the employee has transferred to a different directorate; in accordance with the employee's new job functions and requirements.

5. Guidelines

5.1 General Password Construction Guidelines

- a) A password must have a minimum of 6 characters in length (longer is generally better).
- b) A password must contain at least one alphabetic and one numeric character.
- c) A password must be significantly different from the previous passwords.
- d) A password cannot be the same as the logon username.
- e) A password should not be information easily obtainable about the user. This includes license plate, identity number, telephone numbers, or children's names, etc.
- f) A password must contain both upper and lower case characters (e.g., a-z, A-Z).

5.2 Password Protection

- a) A password must not be revealed to **ANYONE**. (Including Network Administrators or any support staff).
- b) A password must not be disclosed in an email message, voice message or over the internet.
- c) A password may be changed as often as desired.

- d) A password should be as complex as possible, so that no one will be able to guess or identify the password.
- e) A password must never be written on a piece of paper and, or left freely available for other's to see. If the password is written, it must be kept in a secure environment with restricted access.
- e) A user is solely responsible for the safe keeping and integrity of a password. It must be treated in the strictest confidence by the user.

6. Frequency of change of Passwords

- 6.1 The Administrator Account **user name** must be changed every 12 months. The Administrator Account **password** must be changed every 30 days or if there is any indication that the account has been compromised. The new password should be written on a piece of paper and sealed in an envelope that is stored in a safe.
- 6.2 Standard User Account passwords must be changed every 90 days or if the user feels that the account has been compromised. The user still has the discretion to change a password as often as desired.
- 6.3 All new users will have to change their passwords on their first log on to the network.
- 6.4 Password policies are generally set up as standard on the file servers. The server policy will be enforced in line with the written policy. All users must comply with this policy. Should the user not comply with the guidelines, then access to the network or the computer system will be denied.

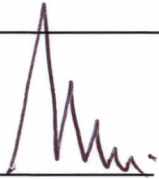
7. General

- 7.1 This password policy should be applied in line with all relevant departmental ICT policies.
- 7.2 Employees should have either a hard copy or electronic soft copy of this policy for reference and guide. The policy can also be obtained from the Government Information Technology Office (GITO).

8. POLICY REVIEW

The policy will be reviewed annually and where need arises.

ENDORSED



HEAD OF DEPARTMENT

18/02/09
DATE

Note: This policy document is a blue print of the original policy that was approved by MEC Justice Piitso on 04.06.07.