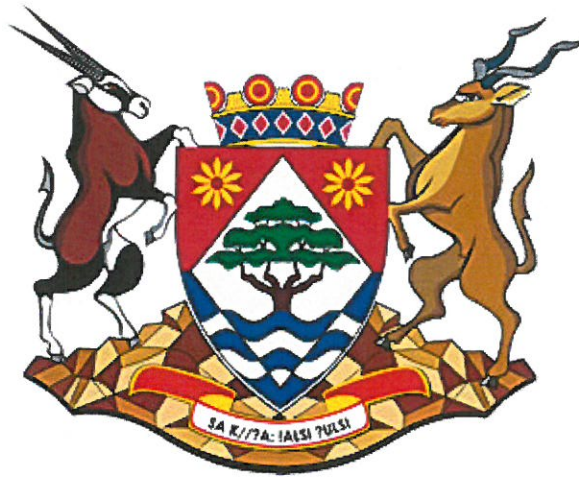
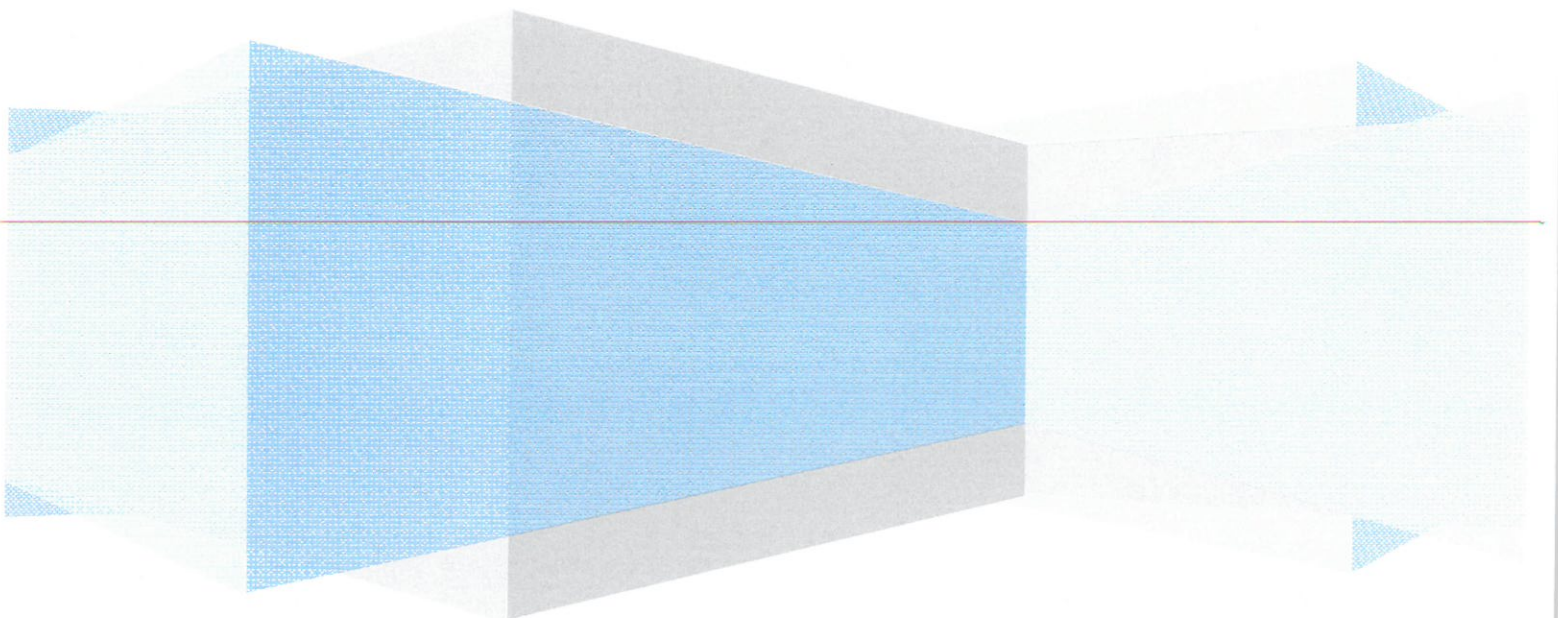


NORTHERN CAPE OFFICE OF THE PREMIER



PASSWORD POLICY VERSION 2.1 2015/16



Document Control

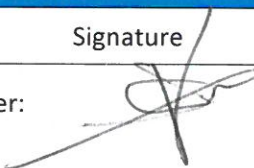
Document Details

Province	Northern Cape
Document	NCOTP Password Policy
Document Name	NCOTP Password Policy 2_1.docx
Document Number:	Version 2
Document Status:	Final
Customer Contact	
Customer Reference:	
File Location:	
Author(s):	

Revision information

Version	Issue date	Author	Reason for Change
1	June 2015	E. Smit	Initial Document
2	May 2019	E. Smit	Revision
3	January 2010	E. Smit	Revision

Document Approval

Name	Designation	Signature	Date	Approval (Y/N)
Mr.C. Vala	Senior Manager: Information Technology		October 2015	Y

INDEX

1. Overview	4
2. Purpose	4
3. Scope	4
4. Policy	4
5. Enforcement.....	6
6. Definitions	6

1. Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Northern Cape Provincial Government's entire network. As such, all Northern Cape Provincial Government employees (including contractors with access to Northern Cape Provincial Government systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3. Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Northern Cape Provincial Government facility, has access to the Northern Cape Provincial Government network, or stores any non-public Northern Cape Provincial Government information.

4. Policy

4.1 General

- 4.1.1 All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.
- 4.1.2 Novell passwords will require a unique password and will be stored in the history list for 200 days.
- 4.1.3 Passwords must not be inserted into email messages or other forms of electronic communication.
- 4.1.4 All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines

A. General Password Construction Guidelines

- 4.2.1 Passwords are used for various purposes at Northern Cape Provincial Government. Some of the more common uses include:
user level accounts, email accounts and screen saver protection. Since very few systems have support for one-time passwords, users should be aware of how to select strong passwords.
- 4.2.2 Poor, weak passwords have the following characteristics:
- The password contains less than eight characters
 - The password is a word found in a dictionary (English or foreign)
 - The password is a common usage word such as:
 - Names of family, pets, friends, co-workers, fantasy characters, etc.
 - Computer terms and names, commands, sites, companies, hardware, software.
 - The words "Northern Cape Provincial Government", "Kimberley" or any derivation based on your physical location.
 - Birthdays and other personal information such as addresses and phone numbers.
 - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
 - Any of the above spelled backwards.
 - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
 - Strong passwords have the following characteristics:
 - Contain both upper and lower case characters (e.g., a-z, A-Z)
 - Have digits and punctuation characters as well as letters e.g., 0-9, !@#\$%^&*()_+|~-
 - =\{'\}[]:~';<>?,./)
 - Are at least eight alphanumeric characters long.
 - Is not a word in any language, slang, dialect, jargon, etc.
 - Are not based on personal information, names of family, etc.
- 4.2.3 Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.
NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

- 4.2.4 Do not use the same password for Northern Cape Provincial Government accounts as for other non-Northern Cape Provincial Government access (e.g., personal ISP account, etc.). Where possible, don't use the same password for various Northern Cape Provincial Government access needs. For example, select one password for the Transversal Access systems such as BAS, PERSAL and a separate password for NOVELL access. Also, select a separate password to be used for any other accounts.

- 4.2.5 Do not share Northern Cape Provincial Government passwords with anyone, including administrative assistants or secretaries.
- 4.2.6 All passwords are to be treated as sensitive, confidential Northern Cape Provincial Government information.
- 4.2.7 Here is a list of "don't's":
- Don't reveal a password over the phone to ANYONE
 - Don't reveal a password in an email message
 - Don't reveal a password to the boss
 - Don't talk about a password in front of others
 - Don't hint at the format of a password (e.g., "my family name")
 - Don't reveal a password on questionnaires or security forms
 - Don't share a password with family members
 - Don't reveal a password to co-workers while on vacation
- 4.2.8 If someone demands a password, refer them to this document or have them call your Information Technology Section.
- 4.2.9 Do not use the "Remember Password" feature of applications (e.g., Outlook, Pegasus). Again, do not write passwords down and store them anywhere in your office.
- 4.2.10 Do not store passwords in a file on ANY computer system (including Laptops or similar devices) without encryption.
- 4.2.11 Change passwords, at least, once every six months. The recommended change interval is every four months.
- 4.2.12 If an account or password is suspected to have been compromised, report the incident to your IT Section and change all passwords.

C. Use of Passwords and Passphrases for Remote Access Users

- 4.3.1 *Access to the Northern Cape Provincial Government Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.*

5. Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Definitions

Terms	Definitions
Application Administration Account	Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).