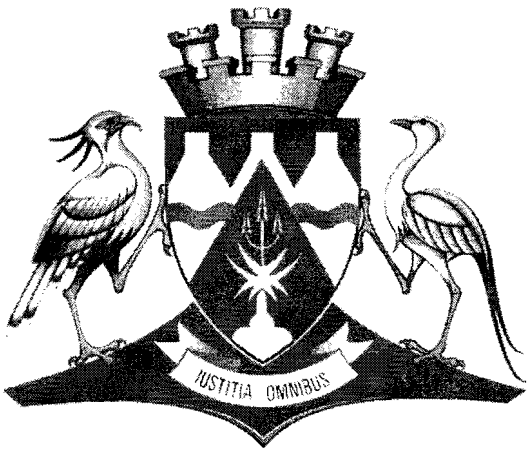
PIXLEY ka SEME DISTRICT MUNICIPALITY



PASSWORD POLICY

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 Pixley Ka Seme District Municipality's entire corporate network. As such, all Pixley Ka Seme District Municipality's employees 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. The policy is intended to reduce the risk of unauthorized access to servers and databases essential to the mission of Pixley Ka Seme District Municipality.

3. Scope

The scope of this policy includes all personnel who have or are responsible for an account (any form of access that supports or requires a password) on any system that resides at Pixley Ka Seme District Municipality or has access to the Pixley Ka Seme District Municipality network information. The policy applies to all users who access Pixley Ka Seme District Municipality's server and databases, including development and test databases, as well as the personal workstation used to access these server and databases.

4. Policy

Unless specifically stated otherwise, the items in this section apply to both end user and system level account and passwords.

4.1 Requirements

The following applies to passwords for system level accounts, application administrative accounts, system administrator accounts, and database administrator accounts

- Each user must have a unique username.
- Accounts associated with passwords that have been expired (persons not in service) for more than 45 days will be deleted

unless there is a business reason to retain the account, e.g. service providers that logs on infrequently.

- Authentication must be to individual users, not groups.
- No passwords are to be stored in clear text.

4.2 Password Guidelines

All users at Pixley Ka Seme District Municipality should be aware of how to select strong passwords.

- The password cannot contain the user's own of close friend's or relative's name, employee number, ID number, birthday, significant anniversary, telephone number, address, or any other information about the user that could be easily guessed or discovered.
- Passwords must not be disclosed to anyone.
- Users should not communicate his, her password or password paraphrase in an email.
- Passwords should not be written down.
- New passwords cannot be a simple change of the previous password, e.g. adding a number at the beginning or end, changing one letter or number.

Strong passwords have the following characteristics:

- Contain at least three of the five following character classes:
  - Lower case characters
  - Upper case characters
  - Numbers
  - Punctuation
  - "Special" characters (e.g. @#$%^&*()_+|~-=\`{}[]:";'<>/ etc)

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 "Pixley Ka Seme District Municipality", "Pixley" or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.

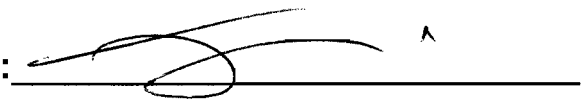
- Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.

4.3 Password Change Requirements

- Passwords should be changed if there is a risk that someone has stolen or guessed them somehow. Changing passwords on a regular schedule can be counterproductive. Regular password changes simply induce people to write their passwords down, or design sequences of passwords, like secret01a, secret01b, etc.
- Passwords must be changed as soon as possible after a compromise and within one business day.
- A password must be changed if directed to do so by the Accountant Computer Services.

5. Responsibility

Users are responsible for protecting their passwords and reporting any compromise promptly to the Accountant: Computer Services.
Users are also responsible for selecting strong passwords (six or more digits, not based on personal information, not a word in any language, contains both upper and lower case characters and have digits included).
Management is responsible for ensuring that users are aware of this policy.

EXECUTIVE MAYOR: 

DATE POLICY APPROVED: **06 SEPTEMBER 2005**

DATE REVISED POLLICY APPROVED : 27 MAY 2016

RESOLUTION: **R 2016 – 05 – 27 (9.7.12)**