# Draft Password Policy

| | |
|---|---|
| Version | 1.0 |
| Draft Date | September 2014 |
| Status | Draft |
| Approved By: | |
| | |

## Contents

## 1.0 POLICY OVERVIEW

Passwords are a very crucial aspect of information and computer security. The use of passwords is the commonest form of authentication for accessing computer systems and the data and information therein. Passwords assure computer system users the first line of defence and protection of their accounts against unauthorized and malicious access to their data and information.

## 2.0 PURPOSE

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

## 3.0 SCOPE

This policy applies to all users who have the responsibility of an account that requires a password to access computers, systems and services and the data and information there in, owned, maintained and hosted by Mbarara University of Science and Technology. The services may be resident on the university's computer network infrastructure or on designated cloud computing platforms.

## 3.0 POLICY PRINCIPLES

### *3.1 General*

1. All system-level passwords (e.g., root, enable, Server admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
2. All production system-level passwords must be part of the Information Security administered global password management database.
3. 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. User accounts that have system-level privileges granted through group memberships must have a unique password from all other accounts held by that user.
5. Passwords must not be inserted into email messages or other forms of electronic communication unless in the case of the issuance of temporal passwords by the Computing Services Unit which would need immediate alteration by the user on receipt.
6. All user-level and system-level passwords must conform to the guidelines described below.

### 3.2 *General Password Construction Guidelines*

Passwords are used for various purposes at Mbarara University of Science and Technology. Some of the common uses include: user level accounts, web accounts, email accounts, screen saver protection, and local router logins. All users should be aware of how to select strong passwords.

Strong passwords have the following characteristics:

1. Contain both upper and lower case characters (e.g., a-z, A-Z)
2. Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
3. Are at least eight alphanumeric characters long.
4. Are not a word in any language, slang, dialect, jargon, etc.
5. Are not based on personal information, names of family, etc.
6. 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.

Poor, weak passwords have the following characteristics:

1. The password contains less than eight characters.
2. The password is a word found in a dictionary (English or foreign)
3. 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.
    - 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)

### *3.3 Password Protection Standards*

1. Passwords used to access MUST services should not be used as passwords for access to other non-MUST services and systems. (e.g., personal email accounts, online banking, NSSF accounts, etc.).
2. MUST account passwords will not be shared with anyone including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential MUST information.
3. MUST account passwords will not be shared with anyone, according to the following guidelines;

   - NOT to reveal a password over the phone to ANYONE
   - NOT to reveal a password in an email message
   - NOT to reveal a password to the superiors, colleagues or subordinates in whatever circumstances.
   - NOT to hint at the format of a password (e.g., "my family name")
   - NOT to reveal a password on questionnaires or security forms
   - NOT to share a password with family members

4. MUST users should never use the "Remember Password" feature of applications (e.g., web browsers, outlook).
5. Passwords should not be written down or stored anywhere. If they are to be stored on computer systems, they should be encrypted.
6. Incidences where accounts or passwords are suspected to have been compromised should be reported to the Computing Services Unit.

### *3.4 Application Development Standards*

Application developers must ensure their programs contain the following security precautions.

1. should support authentication of individual users, not groups.
2. should not store passwords in clear text or in any easily reversible form.
3. should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.
4. should support and be able to work with the university's staff and student directories wherever possible.
5. should consider the guidelines of this policy

### *3.5 Use of Passwords and Passphrases for Remote Access Users*

Access to the MUST Network or services via remote access will be controlled using a one-time password authentication.

### *3.6 Enforcement*

Any employee found to have violated this policy may be subjected to disciplinary action in accordance with the university's Human Resource Policy framework.