PASSWORD POLICY
1. Overview

Passwords are one of the primary mechanisms that protect potentially sensitive official information systems and other resources from unauthorized use. While passwords are not the most secured way of protecting information and information systems, constructing secure passwords and ensuring proper password management is essential. Poor password management and protection can allow both the dissemination of information to undesirable parties and unauthorized access to MLM resources. Poorly chosen passwords can be easily compromised. Password compromise can lead to inappropriate disclosure and use of MLM resources or sensitive information and also disclosure of personal information. Training users in the proper password creation and management greatly reduces these risks.

2. Purpose

The purpose of this policy is to establish minimum rules, guidelines and standards for passwords creation and management used to logon to MLM information systems.

3. Scope

This policy applies to all user accounts provided by MLM and all MLM employees, contractors and service providers that logon to MLM information computers and network.

4. References

i) ISO 17799
ii) Information Security Forum (Code of good practice for Information Security)
iii) Minimum Information Security Standards
iv) Limpopo Information Security Policy
v) Protection of Information Act
vi) International Standard for Risk Assessment
vii) COBIT Audit Framework

5. Policy Statement

All user accounts used to logon to MLM information systems shall be protected with strong passwords. Furthermore, passwords must be changed regularly to avoid unauthorized access to information and information systems. Passwords that are not managed properly are at risk of accidental disclosure overtime.

Requirements

- Every user must have a unique username. For MLM employees this shall be the user’s surname and initials.
- Initial passwords must be uniquely created by a random password generator and must be communicated to the user in a secure
manner. The user must automatically be forced by the computer system to change this initial password upon initial user logon
  _ Passwords may not be blank
  _ To prevent accidental disclosures of passwords and unauthorized access to newly created user accounts, initial passwords can only be changed after a minimum of one day
  _ No passwords will be stored in clear text or reversible encryption
  _ The system administrator in charge of user management will only give initial passwords, unlock accounts or reset passwords once the password reset request form is completed and the identity of the user has been validated
  _ If a user’s password has expired or the user has forgotten the password, then the user must complete a **password reset request form (Appendix A)** and send it to IT Helpdesk for processing. This is to ensure that all requests to reset passwords are recorded for auditing purposes and to prevent unauthorized resetting of other individual’s passwords. I.T Officer may at its discretion require the user requesting the request to physically present him/her self
  _ Passwords used within MLM should not be used for external internet accounts and service providers
  _ Passwords must not be included in any automatic login process.
  _ New passwords may not near any relation to old passwords e.g. password1 and password2

**Password Protection Guidelines**

  _ Never write usernames and passwords on keyboards, walls, monitors, post-it notes, tables or any material. A memorized password is not prone to accidental disclosure
  _ Your password is secure and must not be shared with anyone including but not limited to colleagues, managers and I.T Officers. This exempts generic departmental passwords i.e. passwords used and managed by a group in a specific department
  _ Any file that stores passwords must be encrypted or password protected
  _ New passwords must not be a simple change of the old password e.g. adding a number at the end
  _ Passwords or pass phrases must not be sent via email or communicated verbally except in cases of password resets and initial user creation between I.T Officer and the user involved
  _ Passwords must be changed immediately upon disclosure or suspected disclosure
  _ Passwords may not be written or saved in electronic documents unless these documents are encrypted and the user ensures that the encryption keys cannot be accessed by unauthorized individuals
  _ Computers must be locked when the user moves away from the computer to prevent unauthorized access
Password Guidelines

- Passwords must contain a mixture of special characters, alphanumeric characters in lower and upper cases e.g. P@s$w0Rd can be used instead of password
- Pass phrases can be used instead of highly complex passwords to prevent the need to write the password where it can be accessed by unauthorized individuals, e.g. Take Cover can be converted to T@k3_Cov3r
- Passwords from dictionaries in any language are easily guessable and should be avoided
- Passwords should not be identical to the user ID, names, surname, computer name, job title or anything that a would be password attacker can guess

Password Construction Standards

- Passwords must consist of a mix of special and alpha-numeric characters
- Passwords must not be the same as the username, first name, surname, street address or any words contained in a dictionary of any language

Account and Password Protection

A user account will be locked out indefinitely after three failed attempts in order to protect accounts and passwords from brute force attacks or password guessing. Upon account lockout, only the system administrator can unlock the account at the request of the user involved.

System-Based Password Requirements

Privileged and administrative passwords must be subject to stringent composition and frequency of change. Privilege passwords include passwords for routers, switches, firewalls, IPSes, network operating systems and any other IS resource.

Best Practices for System-Based and Server Passwords

- All Passwords must be documented in the password book and kept in the safe at all times. Only authorized personnel must access the safe. The combination/code for opening the safe must be divided into three unique codes, one for each authorized individual who must be available to open the safe
- Default factory passwords should be changed immediately after installation
- Privileged passwords should not be communicated via telephone, fax, email or any printed form
- Administrator/privilege passwords must not be disclosed to external contractors
- A number of shared local administrative passwords may be used on machines for specific divisions and computer networks
All servers must be configured not to display the last logon username.
Service accounts must not rely on admin accounts$passwords.
Passwords must be unique from all previous passwords.

System Administrators

System administrators and those that have system administrator roles shall configure MLM information systems to comply with this Password Policy. System administrators and information security personnel should work with users in an effort to ensure that they are able to comply with this policy.

Application/Web Developers

Application and Web developers developing applications that require password authentication shall create code that complies with this Password Policy.

Users

Employees, contractors and service providers shall create, maintain and safeguard passwords in compliance to this policy.

6. Enforcement

I.T Officer is responsible for enforcing this policy and continuously ensuring monitoring and compliance.

7. Consequences for Non-Compliance

Any person or entity found to be in violation of this policy may be subject to termination of any access to MLM network.

8. Policy Review

This policy is subject to change from time to time.