Information Security Management System
ISO/IEC 27001:2013

PASSWORD POLICY

POLISI KATALALUAN

For PTM Use Only	Version 1.1	Date: 8th April 2016
Written By: Asiah Abu Samah Pengerusi Jawatankuasa ISMS	**Verified By:** Nor'ain Mohamed Wakil Pengurusan Keselamatan Maklumat (ISMR)	**Approved By:** Dr David Asirvatham Pengarah Pusat Teknologi Maklumat

Revision History

No	Date of Change	Description	Page	Version	Approved By
1	1st October 2014	Remove 'MS' from Front Page.	Front Page	1.1	Dr David Asirvatham
2	25th Nov 2014	Upgrade "Password Guidelines" to "Password Policy"		1.0	Dr David Asirvatham
		Changed Doc No from "UM-ISMS-GL-PTM-002" to "UM-ISMS-POL-PTM-014"			
		Changed the guideline statements to policy statements	2, 3		
		Inserted TERHAD logo	Header		
3	8th Apr 2016	2.0 Scope : edit to system, servers, pc and core network devices	2	1.1	Dr David Asirvatham
		3.2 Password must be changed at least once in every twelve months.	2		
		4.2 Password protection standard – at least once a year	4		
		Remove BM Version	5 - 7		

1.0 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.

2.0 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 UM Centre For Information Technology (PTM)-owned system, servers, pc and core network devices. Each user is responsible for his/her own password(s) used to access the devices/systems under his/her care.

3.0 Policy

3.1 Password stored in digital devices or transmitted via electronic communication must be encrypted (Windows default).

3.2 Password must be changed on a periodic once in twelve months basis.

3.3 An account password can only be known to the account's owner or to users who require access to the account to perform the necessary job function, and no one else.

3.4 All passwords are to be treated as sensitive and confidential information.

3.5 All passwords will be governed by password lock-out control (5 Times) where possible.

3.6 All passwords are advised to conform to the guidelines described below.

4.0 Password Guidelines

4.1 Strong Password Construction Guidelines

Strong passwords have the following characteristics:

- Are at least eight alphanumeric characters long.
- 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 not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- One way to create a strong password is 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.

Poor, weak passwords have the following characteristics:

- The password contains less than six characters
- The password is a word found in any language dictionary
- The password is a common usage word such as:
    1. Names of family, pets, friends, co-workers, fantasy characters, etc.
    2. The word "UM ICT Division" or any derivation.
    3. Birthdays and other personal information such as addresses and phone numbers.
    4. Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    5. Any of the above spelled backwards.
    6. Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

4.2 Password Protection Standards

- All system-level passwords (e.g., root, Windows 2000/XP admin, application administration accounts, etc.) are advised to be changed at least once a year
- All user-level passwords (e.g., email, web, desktop computer, etc.) are advised to be changed at least once a year.
- Do not use the same password for various accounts.
- Do not share password with anyone, including administrative personnel.
- Any request for a password, have them call the responsible person in the respective division
- If an account or password is suspected to have been compromised, report the incident to UMCERT and change the respective password.
- Written password must not be stored in any insecure location (e.g. purse, wallet).
- Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, MSN Messenger).