Information Security Management System MS ISO/IEC 27001:2007

PASSWORD MANAGEMENT POLICY

DASAR PENGURUSAN KATA LALUAN

UNIVERSITI MALAYSIA PERLIS

Written By:	Verified By:	Approved By:
En. Farihan Ghazali IT Officer	Pn. Rohazna Wahab Deputy Director ICT Centre	En. Nasrudin Abd. Shukor Director ICT Centre ISMR

For Dept Use Only

Date: 25th July 2013 **Version 1.1**

Revision History

No	Date of Change	Description	Page	Version	Approved By
1.	15/07/2013	Nama asal Penulis Dokumen iaitu Pn Ummi Naiemah Saraih ditukar kepada En. Farihan Ghazali	0	1.1	Nasrudin Abd Shukor
2.	15/07/2013	Maklumat terkini tentang tempoh penukaran kata laluan pengguna dan tentang emel peringatan dari HOD PC dimasukkan dalam perkara 3.2	4	1.1	Nasrudin Abd Shukor

PASSWORD MANAGEMENT POLICY
DASAR PENGURUSAN KATA LALUAN

1.0 Purpose
1.0 Tujuan

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.

Tujuan dasar ini ialah untuk mewujudkan satu piawaian bagi penciptaan kata laluan yang kukuh, perlindungan untuk kata laluan tersebut, dan kekerapan perubahan

2.0 Scope
2.0 Skop

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 UniMAP ICT Center-owned system and devices. MIS, PC unit, Network, Datacenter is in-charge for user password and server passwords for each of their departments.

Skop dasar ini termasuk semua staf yang mempunyai atau bertanggungjawab untuk akaun (atau sebarang bentuk akses yang menyokong atau memerlukan kata laluan) sistem dan alatan yang dimiliki Pusat ICT UniMAP. MIS, unit PC, Rangkaian, Pusat data bertanggungjawab untuk kata laluan pengguna dan kata laluan server untuk setiap jabatan masing-masing.

3.0 Policy
3.0 Dasar

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

3.1 Kata laluan yang disimpan dalam alatan digital atau disiarkan melalui komunikasi elektronik mesti dienkripsikan (Windows default).

3.2 Password must be changed on a periodic once in 4 months basis. There is an official email from HOD of PC Maintenance Division to all staff to remind the end-user to change the password.

3.2 Kata laluan mestilah diubah secara berkala sekali dalam 4 bulan. Emel rasmi akan keluarkan oleh HOD dari Bahagian Penyelenggaraan PC kepada semua staf untuk mengingatkan pengguna akhir agar menukar kata laluan.

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.

3.3 Kata laluan akaun hanya boleh diketahui oleh pemilik akaun atau kepada pengguna yang memerlukan akses untuk melakukan tugas yang perlu, dan tidak ada orang lain yang tahu.

3.4 All passwords are to be treated as sensitive, confidential information.
3.4 Semua kata laluan akan diperlakukan sebagai sensitif, maklumat sulit.

3.5 All passwords will be governed by password lock-out control. (4 Times)
3.5 Semua kata laluan akan ditadbir oleh kawalan sekat masuk kata laluan. (4 Kali)

3.6 All passwords must conform to the guidelines described below.
3.6 Semua kata laluan mesti mematuhi garis panduan yang diterangkan di bawah.

4.0 Procedure
4.0 Prosedur

4.1 Strong Password Construction Guidelines
4.1 Garis Panduan Pembinaan Kata Laluan Yang Kukuh

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 "UniMAP ICT Center" 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)

Kata Laluan yang tidak baik, lemah mengandungi ciri-ciri berikut:

- *Kata laluan mempunyai kurang dari 6 karakter*
- *Kata laluan adalah perkataan yang dijumpai dalam mana-mana kamus bahasa*
- *Kata laluan adalah perkataan yang biasa digunakan seperti:*
    1. *Nama keluarga, haiwan peliharaan, sahabat, rakan sekerja, karakter fantasi dan sebagainya*

2. *Perkataan "Pusat ICT UniMAP" atau pemerolehan lain*
3. *Tarikh lahir dan maklumat peribadi lain seperti alamat dan nombor telefon*
4. *Perkataan atau corak nombor seperti aaabbb, qwerty, zyxwvuts, 123321 dan sebagainya.*
5. *Mana-mana yang tersenarai di atas yang dieja terbalik*
6. *Mana-mana yang tersenarai di atas yang didahului atau diikuti dengan digit (contoh., rahsia1, 1rahsia)*

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 six alphanumeric characters long.
4. Are not words in any language, slang, dialect, jargon, etc.
5. Are not based on personal information, names of family, etc.
6. 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.

Kata laluan yang kukuh mempunyai ciri-ciri berikut:

1. *Mengandungi kedua-dua karakter kes atas dan bawah (contoh., a-z, A-Z)*
2. *Mengandungi digit-digit dan karakter tanda baca juga abjab (contoh., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)*
3. *Sekurang-kurangnya sepanjang 6 karakter alphanumeric.*
4. *Bukan perkataan dalam apa-apa bahasa, slang, dialek, jargon , dan lain-lain.*
5. *Bukan berdasarkan maklumat peribadi, nama-nama keluarga dan sebagainya*
6. *Satu cara untuk mewujudkan kata laluan yang kukuh adalah berdasarkan kepada tajuk lagu, pengesahan, atau frasa lain. Misalnya, frasa mungkin adalah: "Ini Mungkin Ada Satu Cara Untuk Ingat" dan kata laluan mungkin adalah: "TmB1w2R!" atau "Tmb1W>r~" atau lain-lain variasi.*

4.2 Password Protection Standards

4.2 Piawaian-piawaian Perlindungan Kata Laluan

- All system-level passwords (e.g., root, Windows 2000/XP admin, application administration accounts, etc.) must be changed on at least every 4 months.
- All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every 4 months.
- Do not use the same password for various accounts
- Do not share password with anyone, including administrative personnel.
- If someone demands a password, have them call the responsible person in MIS
- If an account or password is suspected to have been compromised, report the incident to ISMS Implementation Monitoring Committee 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).

- *Semua kata laluan peringkat sistem (misalnya, root, Windows 2000 / XP admin akaun pentadbiran aplikasi dan lain-lain.) mesti diubah di sekurang-kurangnya setiap 3 bulan.*
- *Semua kata laluan peringkat pengguna (misalnya, e-mel, web, komputer meja dan lain-lain.) mesti diubah sekurang-kurangnya setiap 3 bulan.*
- *Jangan guna kata laluan yang sama untuk pelbagai akaun.*
- *Jangan berkongsi kata laluan dengan sesiapa sahaja termasuk staf pentadbiran.*
- *Jika seseorang menuntut kata laluan, minta mereka untuk menghubungi staf yang bertanggungjawab dalam MIS.*
- *Jika akaun atau kata laluan disyaki telah dikompromi, laporkan kejadian tersebut kepada Jawatankuasa Pemantauan Pelaksanaan ISMS dan ubah kata laluan berkenaan.*
- *Kata laluan yang ditulis tidak sepatutnya disimpan dalam mana-mana lokasi tidak selamat (misalnya dompet, beg duit).*
- *Jangan guna ciri aplikasi-aplikasi "Remember Password" (misalnya, Eudora, Outlook, MSN Messenger).*