University Malaysia of Computer Science & Engineering

Password Policy	Created: 01/04/2013
Section of: Corporate Security Policies	Target Audience: Users, CIT
CONFIDENTIAL	Page 1 of 4

University Malaysia of Computer Science & Engineering is hereinafter referred to as "the university".
University network & internet access infrastructure is hereinafter referred to as "UniMyNet".

1.0 Overview

A solid password policy is perhaps the most important security control the university can employ. Since the responsibility for choosing good passwords falls on the users, a detailed and easy-to-understand policy is essential.

2.0 Purpose

The purpose of this policy is to specify guidelines for use of passwords. Most importantly, this policy will help users understand why strong passwords are a necessity, and help them create passwords that are both secure and useable. Lastly, this policy will educate users on the secure use of passwords.

3.0 Scope

This policy applies to any person who is provided an account on the UniMyNet or systems, including: employees, guests, contractors, partners, vendors, etc.

4.0 Policy

4.1 Construction

The best security against a password incident is simple: following a sound password construction strategy. The university mandates that users adhere to the following guidelines on password construction:

- Passwords should be at least 8 characters

- Passwords should be comprised of a mix of letters, numbers and special characters (punctuation marks and symbols)

- Passwords should be comprised of a mix of upper and lower case characters

- Passwords should not be comprised of, or otherwise utilize, words that can be found in a dictionary

- Passwords should not be comprised of an obvious keyboard sequence (i.e., qwerty)

- Passwords should not include "guessable" data such as personal information about yourself, your spouse, your pet, your children, birthdays, addresses, phone numbers, locations, etc.

Creating and remembering strong passwords does not have to be difficult. Substituting numbers for letters is a common way to introduce extra characters - a '3' can be used for an 'E,' a '4' can be used for an 'A,' or a '0' for an 'O.' Symbols can be introduced this was as well: an 'S' can become a ',' or an 'i' can be changed to a '!.'

Another way to create an easy-to-remember strong password is to think of a sentence, and then use the first letter of each word as a password. The sentence: 'The quick brown fox jumps over the lazy dog!' easily becomes the password 'Tqbfjotld!'. Of course, users may need to add additional characters and symbols required by the Password Policy, but this technique will help make strong passwords easier for users to remember.

4.2 Confidentiality

Passwords should be considered confidential data and treated with the same discretion as any of the university's proprietary information. The following guidelines apply to the confidentiality of university passwords:

- Users must not disclose their passwords to anyone

- Users must not share their passwords with others (co-workers, supervisors, family, etc.)

- Users must not write down their passwords and leave them unsecured

- Users must not check the "save password" box when authenticating to applications

- Users must not use the same password for different systems and/or accounts

- Users must not send passwords via email

- Users must not re-use passwords

4.3 Change Frequency

In order to maintain good security, passwords should be periodically changed. This limits the damage an attacker can do as well as helps to frustrate brute force attempts. The university does not wish to apply any hard limits to when passwords must be changed, but asks that users exercise discretion and change passwords sporadically.

4.4 Incident Reporting

Since compromise of a single password can have a catastrophic impact on network security, it is the user's responsibility to immediately report any suspicious activity involving his or her passwords to the Head of Campus IT. Any request for passwords over the phone or email, whether the request came from university personnel or not, should be expediently reported. When a password is suspected to have been compromised the Head of Campus IT will request that the user, or users, change all his or her passwords.

4.5 Applicability of Other Policies

This document is part of the university's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

5.0 Enforcement

This policy will be enforced by the Head of Campus IT and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of company property (physical or intellectual) are suspected, the company may report such activities to the applicable authorities.

6.0 Definitions

Authentication A security method used to verify the identity of a user and authorize access to a system or network.

Password A sequence of characters that is used to authenticate a user to a file, computer, network, or other device. Also known as a passphrase or passcode.

Two Factor Authentication A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

7.0 Revision History

Revision 1.0, 01/04/2013