

IFT Campus Network Password Policy

1. Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of IFT's entire network. As such, all IFT Campus Network account holders are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2. 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.

3. Scope and Applicability

This policy applies to all faculty, staff and students who have or are responsible for an IFT Campus Network account, or who have any form of access that supports or requires a password. This policy applies to any system that resides at any IFT facility, accesses IFT Campus network, or stores any non-public IFT information.

4. Password Construction Guidelines

- 4.1 Initial passwords must be changed at first login;
- 4.2 All passwords must be changed on at least a quarterly basis (90 days);
- 4.3 All passwords must meet the following complexity requirements;
 - 4.3.1 Not contain the user's account name or parts of the user's full name that exceed two consecutive characters;
 - 4.3.2 Be at least six characters in length;
 - 4.3.3 Contain characters from three of the following four categories:
 - 4.3.1.1 English uppercase characters (A through Z)
 - 4.3.1.2 English lowercase characters (a through z)
 - 4.3.1.3 Base 10 digits (0 through 9)
 - 4.3.1.4 Non-alphabetic characters (for example, !, \$, #, %)
- 4.4 If users have forgotten their password, they must contact the IT Helpdesk during normal hours of operation to have the password reset.

5. Password Protection Standards

- 5.1 Do not use the same password for IFT Campus Network account as for other non-IFT access (e.g., Facebook, MySpace, online banking, etc.).
- 5.2 Do not share passwords with anyone, including roommates, student workers, family members, co-workers, administrative assistants or consultants. All passwords are to be treated as sensitive, confidential IFT information.
Here is a list of “dont’s”:
 - 5.2.1 Don't reveal a password over the phone to ANYONE
 - 5.2.2 Don't reveal a password in an email message
 - 5.2.3 Don't reveal a password to the boss
 - 5.2.4 Don't talk about a password in front of others
 - 5.2.5 Don't reveal a password on questionnaires or security forms
 - 5.2.6 Don't share a password with family members
 - 5.2.7 Don't reveal a password to co-workers while on vacation
- 5.3 If someone demands a password, refer them to this document or have them call someone in the Information Technology Team.
- 5.4 Do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including smart phones, PDAs, or similar devices) unless that file is encrypted.
- 5.5 If an account or password is suspected to have been compromised, report the incident to IT Helpdesk and change all passwords.

6. Password Expiration

Users cannot logon to IFT Campus Network if they have not had their password changed within the required change timeframe (15 days before the expiry date).

7. Password Change

During the required change timeframe, the users will be prompted by the system to change password when they log in the campus domain or the users can change it at https://email.ift.edu.mo/IISADMPWD/user_password_change.asp.