Password Security Policy

Purpose

To provide a mechanism to maximize the security of information stored on University technology through the appropriate use of passwords.

Passwords are assigned to each individual as a method to control and monitor their unique access to systems and information, and should never be shared with others.

Policy

Passwords will be changed at least every six months.

Users will change their password immediately upon suspecting it has been compromised.

Users are not to give others access to systems or information by providing them with their account and password.

Users will be held responsible for the actions of others if they have knowingly shared their password and access with them.

Procedure

Where possible, the Center for Information Technology will implement automatic password expiration processes to ensure passwords are changed in a regular and timely manner.

Users should follow the following guidelines when creating or changing a password:

A. make each password unique – do not use the same password for multiple accounts or systems;

B. make the password at least six characters long (the more the better);

C. use at least one special character such as #, $, @, %, etc.; use a mix of upper and lower case;

D. do not use standard words that would be listed in a dictionary (even foreign words) – there are programs designed to break passwords by using all words in a dictionary;

E. do not use simple transformations of words, such as Tiny8 or 7Eleven; and

F. do not use alphabetic sequences such as lmnop.

Enforcement

Violations of any part of this policy may result in disciplinary action as prescribed by University policies and procedures.