Policy Statement
Passwords are an important aspect of computer security. Unauthorized use of passwords may compromise the University’s network.

Statement of Purpose
This policy establishes guidelines for the creation and protection of computer passwords.

DEFINITION
For the purpose of this policy, a “computer password” is a sequence of characters used to determine if a computer user requesting access to a computer system is that particular user.

Applicability
This policy is applicable to all administrators, faculty, staff, students, visitors and individuals outside of the university who use services that have been made available through the University. This policy is applicable to all persons assigned a University computer account.

PROCEDURES
The University has established general guidelines which address selection and authorized use of computer passwords. These guidelines respectively follow.

Selection/Other for Computer Passwords
1. Users will be required to change their password every 90 days.
2. After 3 invalid login attempts, the account will lock for 30 minutes. After the 30 minutes has passed, the account will automatically unlock and you can attempt your login again. (Information Technology will not unlock the account for you!)
3. Your password will need to be complex, meaning that three of the following four rules must apply to your new password:
   a. Uppercase letters
   b. Lowercase letters
c. Number

d. Special character (not a letter or number)

4. Your password cannot contain your Username, First name or Last name.

5. Password must be a minimum length of 8 characters.

To Change Your Password

1. Log onto a campus computer.
2. Press and hold down Ctrl + Alt + Del.
3. When the Windows Security box appears click the Change Password Button. Follow the steps on the screen.
4. The password must meet the password requirements before the password will be changed. Please see the previous page.

Password Management

The following guidelines are offered regarding management of a password.

• Do not share your password with anyone to include your supervisor or colleagues.
• Do not let anyone observe you entering your password.
• Choose a password that is easily remembered so it does not have to be written down.
• Do not send a password through an e-mail message or by telephone.
• Do not hint at the format of a password to anyone (for example, my family name or the number of characters).
• Do not reveal a password on questionnaires or security forms.

PENALTIES FOR UNAUTHORIZED USE OF PASSWORDS

Any individual found to have violated this policy may be subject to disciplinary action as determined by University management. For employees, disciplinary action may be up to and including termination of employment; for students, disciplinary action may be up to and including dismissal from the University.