
SUBJECT: NETWORK AND EMAIL PASSWORD POLICY

PURPOSE: 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 compromising of the university's entire network. All university employees are responsible for selecting and securing their passwords. All students are initially assigned a user ID and password. Each student is responsible for changing and securing his or her password.

GENERAL POLICY

1. All user IDs and passwords will be unique to each authorized user.
2. Passwords will consist of a minimum of six (6) alpha-numeric characters. Common names and/or phrases may not be used.
3. Passwords will be kept private. Passwords may not be shared, coded into programs or written down.
4. Passwords will automatically expire after 90 days. All users will be required to change their password at this time.
5. A user account will be "frozen" after five (5) failed login attempts.
6. Administrative system sessions will be suspended after sixty (60) minutes of inactivity. A password will be required to log back in.
7. Successful logons should display the date, time, and location of the last successful logon.
8. All user IDs and passwords will be terminated within seven (7) working days of discontinuation of employment.
9. Student accounts will remain active as long as a student maintains continuous enrollment.

PASSWORD AUDITING

All user IDs and passwords are susceptible to periodic auditing for weakness. All users found to have weak passwords will be notified and given three (3) days to change their password, otherwise the account will be suspended.