Password Guidelines

The purpose of this document is to establish the creation of acceptable password selection and maintenance. It provides guidance on creating and using passwords in ways that maximize security of the password and minimize the misuse or theft of the passwords that could lead to a compromised account. Users are responsible for taking the appropriate steps to use strong passwords, as outlined below.

PASSWORD GUIDELINES

- Passwords must be at least 8 characters in length.
- Must contain at least 3 non-alphabetic characters (e.g. $, %, &, #, !, 1, 2, 3).
- Employee and student passwords must be changed every 180 days.
- Never share your password with others.
- Passwords should never be written down or be viewable in open areas.
- Passwords should never be emailed.
- Never reuse passwords.
- An example of a secure password is "TmB1w2R!" or "Passphrases Are Good4 Security2!".
- If an account is suspected to have been compromised, report the incident immediately to the Information Technology Department and change all passwords.

ACCOUNT LOCKOUT

If an individual fails to enter the correct password after three attempts, his or her user account is locked out for 15 minutes. After a period of 15 minutes the user account is automatically unlocked in which the account can be used again.