Password Best Practices and Security Requirements

Jeff Clark - 2018-04-02 - Accounts and Access

# Password Best Practices and Requirements

FAU is committed to the highest integrity in securing its IT environment. Your FAUNet ID and your password is the University's standard for authentication for most information systems.

## FAU Account Security Requirements

Passwords must be 8 to 30 characters in length.
Passwords should contain a mix of uppercase letters, lowercase letters, numeric digits, and symbols (at least 3 of the 4 classes).
Passwords should not contain your username, first name, or last name.
Passwords must not repeat your last 6 password.
User accounts with passwords older than 1 year will be required to change their password at next login.
Users will be notified 30 and 15 days prior to their password expiring and be allowed to change the password.

## Recommendations for a Secure Password

Use a combination of upper- and lowercase letters, numbers, and symbols (e.g., @ & $ ! # % ^ + - ).
Never use your username as your password.

Never use any form of your name, pet's name, or other name readily associated with you.
Never use a word found in the dictionary.
Change your password regularly, at least every 180 days.

## How do I change my password?

Students, Faculty, and Staff can change their password at the FAU Account Self-Service portal and click on "Manage Your FAU Account" link. Provide your FAUNet ID and current password. Then click "Change Your Password" link to reset your password.

Users already logged into Microsoft Windows can use Ctrl + Alt + Del and select the "Change Password" button.

## To Keep Your Computer and Accounts Secure

Use password-protected screen savers (on a PC, go to Start --> Control Panel --> Display; select the Screen Saver tab, and check the box for 'On resume password protect').
When you leave your desk, always lock your computer (ctrl-alt-del) or log off so your computer is protected by your password while you are away.
Do not place your password on a Post-It note taped to your monitor, under your keyboard, or anywhere in your desk.
Do not share your password.
Use long, easy-to-remember passwords. A longer password is much more difficult to break than a shorter password with a higher level of complexity.

## Examples of Good Passwords

!0n3yM4n This variation of 'moneyman' uses the recommended

combination of upper and lowercase letters, symbols (punctuation), and numbers for letters.
Env$43tyR0ck! This example is more than 9 characters long, uses numbers, punctuation, and a mix of upper- and lowercase letters.
Sp4c3_Eng_D3$1gn3r This password consists of three words, separated by punctuation, and uses upper- and lowercase letters and numeric/symbol substitution.