Password Guidelines

One of the first steps to securing information is to assign a strong password. The purpose of these guidelines are to set a standard for creating, protecting, and changing passwords such that they are strong, secure, and protected.

Assigning a strong password

When assigning a password, passwords must comply with standards set forth in the University's Password Policy.

Passwords should NOT contain

When setting up a password, users tend to use a password that's easy for hackers to guess, it's important to develop a strong passwords that are NOT easily guessed. The following are items that should NOT be apart of a password.

- Personal information (ex. Name, nickname, pet's name, child's name, etc.)
- Sequential number (ex. 123456) or letters (ex. abcdef)
- Keyboard patterns (ex. qwerty or asdfg)
- Words associated with your school (ex. UST, Celts)
- Word in the dictionary
- Blank Spaces

Technique for creating a strong, secure password

When creating a password, it is important to think of password that is complex, but familiar with the user. Listed below is an example of creating a strong, secure password.

When creating a password, it is important to think of password that is complex, but familiar with the user. Listed below is an example of creating a strong, secure password.

- Choose a sentence or phrase only you know. Ex. "I Always Eat Burgers on Saturday at the Park"
- Use the first letters of each of the words of the sentence. Ex. "iaebosatp"
- Substitute number and special characters for some of the letters. Ex. "! @lways Eat burgers 0n $aturday @t the Park" would become "!@Eb0$@tP"

Safeguard your passwords

A good password is secure a password; one that is not shared with anyone. When sharing your password with others, that user puts information that is protected by that password at a greater risk. Passwords also help to determine accountability for all transactions and other changes made to system resources, including data. If you share your password with a colleague or friend, you may be giving an unauthorized individual access to the system and may be held responsible for their actions.

- A secure password is one that is not posted, or written down. Experience hackers know to look for exposed passwords that are posted on monitors, hidden under keyboards, and or even in a desk drawer.
- A secure password is one that is never sent via e-mail; when e-mailing your password, that user puts information at risk, which can be seen by other or intercepted by experienced hackers.
- When receiving a default password, always change it immediately, the user must make the password complex yet, easy to remember by following the guidelines, mentioned earlier.
- A secured password should be changed regularly. Experienced hackers will find ways to decrypt your password, it's important for the user to get into the habit of changing passwords regularly.
- A secure password should never be used for critical services as well as for unofficial, off-campus, or social networking sites. Experienced hackers are able to associate the user's password that they use off site with more critical sites, in which, they could access.