Chabot • Las Positas Community College District

Information Technology Services

Password Guidelines

Passwords are the keys to system security, and they provide the most important defense against unauthorized use of District systems. Under CLPCCD Administrative Rules and Procedures 2311, each system user is responsible to

- follow certain rules when creating passwords
- select passwords that are secure
- change login passwords periodically
- keep passwords secret

Users must follow certain rules when selecting passwords. Each user of the Banner administrative systems must select a password for access to the IBM computer, and a second password for access to the Banner *PROD* (production) database.

IBM passwords must be 6, 7, or 8 characters long and must include a number or other special character such as * or + or %. For example, you might choose *bait%hog* as a password. Please remember that IBM, Banner and Netware login passwords are case sensitive (that is, *Muxtri3* is not the same as *muxtri3*), so you must pay attention if you choose to capitalize any portion of your password. Also, please don't forget your password. ITS cannot look it up for you because passwords are stored on the system in an encrypted form. If you forget, we'll have to reset your password and allow you to choose a new one.

Banner database passwords can vary in length dependent on access method and are not case sensitive. Numbers and special characters are allowed, but not required. It is often convenient to make your Banner database password identical to your IBM login password, and to change both when prompted by the system.

If you use the local area network, you also will have a password for login to it. Local area network passwords must be at least 5 characters long and are case sensitive. Again, numbers and special characters are allowed, but not required.

Users must select secure passwords. Good passwords are memorable but unlikely to be guessed. Certain common errors result in passwords that are easily guessed and vulnerable to hackers who may attempt unauthorized use of your account.

Don't choose a password based on any of the following sources:

- your own name, nickname, or any other person's name
- any name spelled backwards or with a number added (e.g. *bill92*)
- any form of your IBM login account name (doubled, reversed, capitalized, etc.)
- any word contained in a dictionary or any familiar word (e.g. *library* or *hayward*)
- information easily obtained about you (e.g. telephone number, license plate number, brand of auto, home street name)

These prohibitions may sound restrictive, but secure, memorable passwords may be chosen by several proven methods:

- Choose two short words and join them together using a special character. Also, mix in some capitals. (e.g. *Bun$Club)*
- Alternate between a consonant and one or two vowels up to eight characters. This method can create nonsense words that are easy to pronounce and remember.
  (e.g. *mowama97*)
- Choose a line from a poem or song and use the first letter of each word. For example, "@Fog Crept In On Little Cat Feet" becomes *@FCIOLCF*.

Users must change passwords periodically. You may change your IBM, or Banner database passwords at any time by making selections from the IBM login menu. In addition, for security reasons, you will be forced to change your IBM password when it expires after three months.

When changing your password, you will be prompted for your old password and then your new password. You will be asked to retype the new password to ensure that you did not make at typing mistake.

Local Area Network (LAN) users: You may change your password for the LAN at any time by pressing Control-Alt-Delete and selecting Change Password

Users must keep passwords secret. Correct password practices are essential. Passwords must be kept secret! Memorize your password; don't write it down. Never store your password in a desk drawer or file where it might be discovered. Never allow anyone else to use your password, regardless of that person's integrity or position. Never give your password over the phone to anyone, even if they claim to be from ITS. Many system and database events are audited by user password, and you will be held responsible for all activity under your password.

System security depends on you!

Revised 7/27/01