How to change your passphrases - Mac

Your new passphrases, PIN, and voicemail password can be found on the yellow Information Sheet. You should change these as soon as possible. As a Calvin faculty or staff, you are responsible to protect sensitive information. This includes your personal private information, college confidential information, and community information. The easiest way to do this is with a good passphrase. For the definition of sensitive information please see Appendix B of the Policy for Responsible Use of Technology at http:// http://www.calvin.edu/it/itpolicies/AUP.pdf
Note: Your Novell and KnightVision passphrases expire every 365 days. You will receive an email reminder prior to the expiration date.

Novell (network access and printing)

Your Novell passphrase is used to login to the Novell network, iPrint (network printing), NetStorage (off-campus network access) and GroupWise.

1. Go to www.calvin.edu/it and click on **Change Novell passphrase** in the menu on the right.
2. When you change your passphrase for the first time you will be prompted to set a secret question and answer so that when you need to reset your password/ passphrase you can do it yourself without help from CIT.

GroupWise (email)

1. Your GroupWise passphrase is the same as your Novell passphrase.

KnightVision (Course management tool and college portal)

Your KnightVision passphrase is also used for *CalvinWireless* (wireless access), Colleague (college database), and KnightVision Services.

1. To change your KnightVision passphrase go to www.calvin.edu/it
2. Select **Change KV Passphrase** from the menu on the right.

PIN (building access)

1. To change your PIN, go to www.calvin.edu/it.
2. Select **Change PIN** from the menu on the right.

Voicemail

The Audix automated voicemail system does not provide prompts to change your password. To change your password:

1. Login to Voicemail by pressing the **VMail** button on your telephone.
2. You are prompted to enter your five-digit phone extension and the # sign.
3. You are prompted to enter your current password and # sign.
4. When you hear the automated system start to give you account options press **5** and then **4**.
5. You are prompted to enter a new password then press **#**.
6. You are prompted to re-enter your new password and then press **#.**
7. Press ****9** to exit Audix.

Passphrase requirements for Novell, KnightVision and GroupWise

- must be a minimum of 15 characters long
- must use characters from two or more of the following groups:
  - Lowercase characters
  - Uppercase characters
  - Number characters

Please talk to your supervisor or departmental chair if you need access to other systems.
*Please see the back for passphrase requirements and good security habits

    - Symbol characters and Spaces
- must include at least 4 different characters
- may not repeat the same character 3 times sequentially
- may never be reused
- will expire in 365 days

Good security habits

Whether it is someone trying stealing an exam, your passphrases, or gaining access to your hard drive or network information, it is important that you protect your computer from these threats.

- It is your responsibility to make sure that all your account passphrases/ passwords are as secure as possible. That includes creating a secure secret question with an answer that only you know the answer to. The answer to your secret question is not case sensitive and ignores punctuation.
- Do not share your passphrase. Sharing your passphrase is against the Policy on Responsible of Technology and could result in disciplinary action.
- Do not use a default passphrase assigned by someone else.
- Do not write your passphrase down in a place where others could find it.
- Be sure no one is watching when you login using your passphrase.
- If you enter a passphrase into a web site, be sure log off the site and then close all open browser windows when you are done.
- Do not use Internet Explorer's (or other programs) Auto Complete or Remember Passphrase function for usernames and passphrases.
- Lock your computer with a screen saver passphrase. http://www.calvin.edu/it/services/training/os/
- Store private and confidential information on a network drive.
- Shut down your computer down at night.
- Shield your computer screen from displaying confidential information from people not authorized to view that information.
- Protect printed private and confidential information. Documents containing confidential information should be locked in a storage cabinet. These confidential documents should be shredded when you no longer need them.
- Only use secure connections when sending confidential information over the internet or by email. Email to students or off-campus addresses is not secure.
- Protect confidential information stored on any portable electronic medium (e.g., laptop, CD, DVD, USB drive, "thumb drive", etc.) While information stored in KnightVision, Novell, Colleague and Benefactor is secured by a passphrase, information stored on your local hard drive or any portable electronic device is not. ***If you are storing confidential information on your hard-drive or any portable electronic device it MUST BE protected using encryption.*** To add data encryption to your device, please contact the HelpDesk at x6-8555.