BELMONT ABBEY COLLEGE
OFFICE OF INFORMATION TECHNOLOGY POLICY AND PROCEDURES

Do not expire
Date Issued: **10/01/2014**
Reviewed/Revised:

PROCEDURE: PASSWORD POLICY

1.0 Overview
Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Belmont Abbey College's entire corporate network. As such, all Belmont Abbey College faculty, staff and employees (including contractors and vendors with access to Belmont Abbey College systems) are responsible for taking the appropriate steps to select and secure their passwords.

2.0 Purpose
The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope
The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Belmont Abbey College facility, has access to the Belmont Abbey College network, or stores any non-public Belmont Abbey College information.

4.0 Policy
4.1 General
- All system-level passwords (e.g., root, enable, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the Office of Information Technology (referred to as IT) administered global password management database.
- All user-level passwords (e.g., email, web, desktop computer, etc.) do not expire.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines
A. General Password Construction Guidelines
Passwords are used for various purposes at Belmont Abbey College and everyone should be aware of how to select strong passwords.

Strong passwords have the following characteristics:

- Are at least 20 alphanumeric characters long.
    - Use 4 or 5 random words
    - Use truly random words; do not use a phrase from a book, movie, or song.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.

- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Current Password Construction
Belmont Abbey has adopted the following characteristic standards for Active Directory (College desktop login, email and MyAbbey/Self-Service) passwords effective October 2014:

- Are at least 20 alphanumeric characters long.
    - Use 4 or 5 random words
    - Use truly random words; do not use a phrase from a book, movie, or song.
- You may not use one of your last 24 passwords

C. Password Protection Standards
Do not use the same password for Belmont Abbey College accounts as for other non-Belmont Abbey College access (e.g., personal ISP account, option trading, benefits, etc.). Do not share Belmont Abbey College passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Belmont Abbey College information.

Here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password in an email message
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Information Technology Department.

The Information Technology department will NEVER ask for your password in an email, if you receive such an email STOP and forward a copy of the email to the help desk at support@bac.edu

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

If an account or password is suspected to have been compromised, report the incident to IT and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by IT or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

D. Sharing User IDs or Passwords

It is strictly against Belmont Abbey's password policy to share user IDs or passwords amongst staff. Remember, you are responsible for all actions taken with your ID and all events are logged.

Each person should have their own user ID and password unless expressly authorized in writing by the University CIO.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.