Bethany Lutheran College, Inc.

PASSWORD POLICY

Purpose and Scope

The purpose of this policy is to protect confidential information vital to College business. Password complexity and rollover will help prevent individual user accounts and the information contained therein from being compromised by others.

The scope of this policy applies to all employee accounts in the Bethany Lutheran College, Inc. domain and other systems that contain confidential data.

Password Requirements

Complex passwords will be required by all employee accounts in the Bethany domain and other systems that house confidential data before the information in those accounts can be accessed.

1. All passwords must be at least eight characters in length (twelve characters or more for members of the ITS department).
2. Passwords must not have been used in the four previous passwords.
3. Passwords must not contain the individual's name or account name.
4. Passwords must contain at least three of the following four character groups
    - English uppercase characters (A through Z)
    - English lowercase characters (a through z)
    - Numerals (0 through 9)
    - Non-alphabetic characters (such as !, $, #, %)

Other Requirements

Since passwords are a major security tool to protecting valuable College information, it is in violation of this policy to:

1. share your password with others (both employees or non-employees).
2. openly display your passwords in your working area.

Minimum Frequency of Change

- Administrative passwords for servers – quarterly (responsibility of the ITS department)
- Administrative passwords on non-server computers – annually (responsibility of the ITS department)
- ITS department staff – quarterly (responsibility of the employee)
- Staff with access to Administrative software products (Jenzabar, PowerFaids or Kronos) – semiannually (responsibility of the employee)
- Staff and Faculty without access to the administrative software mentioned above - annually

If individuals desire to change their passwords more frequently than is outlined here, they are encouraged to do so. If at any point, an individual believes the security of their password has been compromised, they must change their password immediately rather than waiting for the next cycled change.

Enforcement

Anyone found to be in violation of this policy may be subject to appropriate disciplinary action including termination of employment.

See also the Administrative Data Policy for further security information.