POLICIES AND PROCEDURES
Southern Nazarene University

NUMBER:
TITLE: Password Policy
DATE IMPLEMENTED: In place as of 3/18/2013
RESPONSIBLE ENTITY: Information Technology
APPLICABLE TO: All SNU students and employees

POLICY: 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 Southern Nazarene University's entire network. As such, all Southern Nazarene employees (including contractors and vendors with access to Southern Nazarene University's systems) and students are responsible for taking the appropriate steps, as outlined below, 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 and students 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 Southern Nazarene University facility, has access to the Southern Nazarene University network, or stores any non-public Southern Nazarene University information.

4.0 Policy

4.1 General

- All system-level passwords (e.g., application administration accounts, domain admin, etc.) must be changed at least every six months.
- All production system-level passwords must be part of the IT administered global password management database.
- All user-level passwords (e.g., email, web, etc.) must be changed at least every twenty-four months.
- User accounts that have system-level privileges granted through group memberships or programs must have a unique password from all other accounts held by that user.
- 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 Southern Nazarene University. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, and voicemail passwords. Everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password contains less than eight characters
- The password is a single word found in a dictionary (English or foreign)
- The password is a common usage word such as:
    - Names of family, pets, friends, co-workers, fantasy characters, etc.
    - Computer terms and names, commands, sites, companies, hardware, software.
    - The words “snu”, “bethany”, “oklahomacity” or any derivation.
    - Birthdays and other personal information such as addresses and phone numbers.
    - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
    - Any of the above spelled backwards.
    - Any of the above preceded or followed by a digit (e.g., secret1, 1secret)
- The password is the default password for a newly created account

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z) if system permits.
- Have digits and special characters as well as letters (e.g., 0-9, ! @ # $ % ^ & * ( ) _ + | ~ = \ } { [ ] : ” ; < > ? , . /) if system permits.
- Are at least eight alphanumeric characters long if system permits.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored unencrypted.

B. Password Protection Standards

Do not use the same password for Southern Nazarene University accounts as for other non-SNU access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don’t use the same password for various Southern Nazarene access needs.

Do not share Southern Nazarene University passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, confidential Southern Nazarene University 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 at ext 6396.

Do not use the “Remember Password” feature of applications (e.g., mail clients, web browsers).

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 mobile devices) without encryption.

If an account or password is suspected to have been compromised, report the incident to the IT department and change all passwords. It is NOT the responsibility of the IT department if data is compromised because of password violations.

This policy applies to the Southern Nazarene University networks via remote access as well.

IT or its delegates may perform password analyzing on a periodic or random basis. If a password is found unacceptable on one of these scans, either the user will be required to change it or the account will be disabled.

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions. Applications:

- Should support authentication of individual users, not groups.
- Should not store passwords in a clear text of in any easily reversible form.
- Should provide for some sort or role management, such that one user can take over the functions of another without having to know the other's password.
- Should use encryption via SSL/TLS standards for password transmission

5.0 Enforcement

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