PASSWORD POLICY

2016 - 2017

JANUARY 19, 2016

NEWBERRY COLLEGE
2100 College St., Newberry, SC 29108

Contents

1.0 Overview

Passwords are a vital aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password can compromise Newberry College's data systems and services. As such, all users (including contractors and vendors with access to Newberry College's systems) are responsible for taking the appropriate steps, outlined below, to select and secure their passwords.

2.0 Purpose

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

3.0 Scope

The scope of this policy includes users who meet any of the following criteria:

- Users responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Newberry College facility
- Users with access to Newberry College's network
- Users who store any non-public Newberry College information.

4.0 Policy

4.1 Guidelines

A single user sign on process is used for Email, Wolf Den, and Network access. All systems have synchronized user names and passwords and this information is maintained in one location. Under this policy faculty and staff will be required to change their passwords every 180 days. In terms of password administration, the following list provides requirements for establishing and maintaining passwords:

1. Passwords must be a minimum of seven characters in length.
2. Passwords must contain characters from three of the following four categories:
    a. Uppercase Alphabetical letters (A-Z)
    b. Lowercase Alphabetical letters (a-z)

c. Digits (0-9)
d. Nonalphanumeric characters: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/

Examples: Passed12!, paSSw0rd, pA12x4cc

3. Passwords must not contain the user's entire login name or entire full name.
4. Passwords must not include spaces.
5. Passwords should be memorized. Passwords are not to be written down or stored by other means.
6. Passwords should not be shared with anyone for any reason. Please see the Newberry College Acceptable Use Policy for enforcement and penalties.
7. Users need to change their password prior to the expiration date. Upon expiration they will be locked out of Email, Wolf Den, and Network access.
8. Re-using previous passwords: new passwords must differ from the 3 previous passwords.
9. Account lockout: after three failed attempts to log in, a user account will be locked out for five minutes.
10. Login notification reminders will be sent to users 5, four, three, two and one day before the passwords expire (via email on the 5th day before as well).
11. For more advanced details on the guidelines, see Appendix.

If you have any question regarding changing your password, please call OCT at ext. 5646, or 803-321-5646, or via email oct@newberry.edu.

4.2 Password Protection Standards

Password protection is a vital part of any security plan please observe the following standards:

- Do not use the same password for Newberry College accounts as for other non-Newberry College accounts, such as personal ISP account, benefits, banking, and other accounts.
- Do not share Newberry College passwords with anyone, including administrative assistants or secretaries.
- All passwords are to be treated as sensitive Newberry College information.
- When IT works on your computer, please arrange to be available to type in your password as needed. If that is not possible, change your password immediately before and after the work is done.

- Good practices to follow:
    - Don't reveal a password over the phone to ANYONE
    - Don't reveal a password in an email message to ANYONE
    - Don't reveal a password to a supervisor
    - 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 to ANYONE
    - Don't share a password with family members
    - Don't reveal a password to co-workers (e.g., when going on vacation or leave of any kind)
    - Don't use the "Remember Password" feature of applications to store Newberry passwords.
    - Don't store passwords in a file on ANY computer system (including Smartphones or similar devices) without encryption.

5.0 Enforcement

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

6.0 Advanced Group Policy Settings

Setting	Value	Value
Enforce password history	number of passwords to remember	3
Maximum password age	number of days before a password expires	180
Minimum password age	minimum number of days a password should not be changeable	7
Minimum password length	length of password	7

Passwords must meet complexity requirements	Enable/Disable whether password should be complex or not	Enabled
Account lockout duration	Number of minutes a locked-out account remains locked out before automatically becoming unlocked	5
Account lockout threshold	Number of failed logon attempts	5
Reset account lockout counter after	Number of minutes that must elapse after a failed logon attempt before the failed logon attempt counter is reset to 0 bad logon attempts	60