Wells College
Information Technology Policies
Password Policy

(Approved August 2, 2017)

Policy Statement

Wells College protects its computers, systems, and data through user account credentials. It is the user's responsibility to protect these credentials. The user's password is an important part of computer security at Wells College. They often serve as the first line of defense in preventing unauthorized access to campus computers, systems, and data.

Purpose

Wells College has established this policy to ensure all college resources receive adequate password protection by standardizing the requirements to all users of the college network systems. Passwords must be complex and cryptic enough to prevent others from guessing them or hacking them. Passwords must be kept secret and secure, so others can't use them or find them.

User accounts are classified by the type of data the user can access on the network, as those who can access Personally Identifiable Information (PII) or Sensitive Personal Information (SPI) or Financial Information or those who administer applications shall have more restrictions applied to them. "General Users" would include students and staff that have no access to shared network resources. "Standard Users " have access to shared network resources but cannot access sensitive data. "Secure Users" have access to sensitive data as defined by State and Federal Regulations. This password policy will outline rules for each user classification.

Users of the Well College computer systems must agree to the terms and conditions outlined in this policy and other college policies in regards to using the Wells College network, email and computer systems on campus. As with other College policies, violation of the Password Policy can result in disciplinary action.

Scope

The Wells College Password Policy applies to all staff, students, and faculty of the College.

Expectations

a) **Passwords must be complex.**
Passwords must meet the following requirements: Passwords cannot contain the user's account name or parts of the user's full name that exceed two consecutive characters. Passwords must be at least eight characters in length. Passwords must contain

characters from three of the following categories: English uppercase (A through Z), English lowercase (a through z), base ten digits (0 through 9), Non-alphabetic characters (for example,!,$,#,%). The Active Directory Network at Wells College will remember the last three passwords used, and they cannot be reused; this may not be the case with some application passwords.

b) **How to create a strong password.**
To create passwords that are complex, but easily remembered; one way to do this is to create a password based on a song title, affirmation, or another phrase. For example, the phrase might be: "This may be one way to remember," and the password could be: "TmB1w2R!" or some other variation.

c) **System-level passwords.**
System-level passwords must conform to the same guidelines as user-level passwords.

d) **Change passwords often.**
Passwords should be changed often. At Wells College passwords shall expire as follows: General Users shall have no account expiration or required password change period. However, all users shall be asked to change their password on their very first log on. Standard Users will have their password expire every 120 days. Privileged Users, which include System Administrators will be required to change their passwords every 90 days.

e) **Do not share passwords.**
Passwords should never to be shared with anyone else. Anyone with a need to access the computers or network resources at Wells College shall be provided with unique credentials. Passwords should not be written down and hidden under keyboards or posted or stored near workstations. Passwords should never be inserted into an email or another form of electronic communication.

f) **Compromised passwords.**
If a user's password is compromised or suspected of being compromised, the password must be changed immediately. Passwords can be changed at the Wells College Single-Sign-On portal or from Office365 online.

g) **Lost credentials.**
If credentials are lost, they account holder must show proof of their identity before IT personnel can issue new credentials or reset passwords. A user may change their password through the online portals if they have previously set up security questions and answer those correctly.

h) **Protect your credentials.**

All users should take steps to avoid phishing scams and other attempts by hackers to steal passwords or other sensitive information. All employees will receive training on how to recognize these attacks and will be periodically tested with internal phishing attack tests. Those falling for the Phishing will be subject to more frequent testing and will be sent training materials to help them understand the risks of falling for Phishing.

i) **System protection against hacking.**
In the event of 3 or more attempts to log onto an account unsuccessfully, a user's account shall be locked out for thirty minutes in case the failed login attempts were the result of a hacking attempt.