Information and Technology Services Policies

Section 811: Access Control Policy	Policy Number: 811.0 Password Policy
New: __X ___ Revised: ___	Effective Date: August 1, 2015 Last Day Reviewed:
Scope: Faculty, Staff, and Students	Authority: Information and Technology and Services

811.0 Title Password Policy

811.1 Purpose

Otterbein University relies on the use of University provided credentials (User name and password) to provide access authentication to online information technology resources such as email, institutional data, University websites, academic and personal data, cloud computing processes, and other sensitive services. In particular, passwords are the user's 'keys' to gain access to University information and information systems. A compromise of these authentication credentials directly impacts the confidentiality, integrity, and availability of IT systems, and University as well as user information. This policy establishes minimum standards for the creation and protection of each person's University password(s). All users accessing Otterbein's IT resources are bound by the requirements as described in this policy, to create and secure their password(s).

811.2 Scope

This policy applies to all Otterbein IT systems and resources that require password authentication. All system administrators and users of University IT resources are responsible for implementing and maintaining the requirements outlined in this document. Policies and/or standards adopted by a school or administrative unit must be consistent with this policy, but may provide supplemental controls, guidelines, and further restrictions.

This policy also applies to certain non-Otterbein IT systems accounts, such as cloud computing applications, that provide access to sensitive University information and information systems where the exposure may have significant impact on University operations. Do not use the same password for Otterbein accounts as for other non-Otterbein access, such as, online banking, personal ISP accounts, Facebook, MySpace, Twitter, or other social network accounts. This policy does not apply to password-protected files, encryption key passphrases, or local accounts that do not interface with Otterbein user account authentication systems (LDAP, Active Directory, and Azure AD).

811.3 Policy Statement

Individuals must have a unique identifier and password for each University account.

- All Otterbein owned electronic devices that access confidential/restricted University data must have password protection enabled.
- Passwords must be stored in irreversible encryption format whenever possible.
- Passwords must contain at least eight (8) characters and contain characters from three of the four categories below:

1) At least one upper case alphabetic character
2) At least one lower case alphabetic character
3) At least one numeric character (1, 2, 3, etc.)
4) At least one punctuation or symbol character (@, $, #, etc.)

Note: Do not use ‘ “ or blank spaces as they may not work with University systems

- Faculty, staff, and student passwords must be changed at least once every six months
- Passwords cannot be set to one of the previous 5 passwords
- Administrator user accounts that have system-level privileges granted through group memberships must have unique passwords for each account(s) held by that user.
- The IT Help Desk and system administrators must verify the identity of users when assigning or resetting passwords.
- All vendor supplied default passwords must be changed prior to any application or program's implementation to a production environment.

811.4 Enforcement

Information and Technology Services has the responsibility to enforce this policy through systematic means and/or departmental network administrators, IT system administrators, and system users. All Otterbein employees are responsible for complying with this policy. Failure to comply may result in disciplinary actions.