# Password Policy

**Section**: 60.1

**Section Title**: General IT Guidelines

**Approval Authority**: Board of Trustees

**Responsible Executive**: Executive Vice President

**Responsible Office**: Office of Information Technology

**Originally Issued**: N/A

**Revisions**: 5/22/2015

**Policy Summary**: This policy describes the University's requirements for acceptable password selection and management to maximize security of Personally Identifiable Information (PII) and University data.

**Reason for Policy**: To establish password guidelines that will maximize the security of Personally Identifiable Information (PII) and other sensitive or valuable University data.

**Related Documents**:

- N/A

**Policy**:

## Purpose

This policy describes the University's requirements for acceptable password selection and management to maximize security of Personally Identifiable Information (PII) and University data.

## User Passwords:

- Passwords should never be shared with anyone for any reason.
- Domain user passwords will be managed by the University's Password Manager application (mypassword.highpoint.edu) and must meet the password strength criteria established within the system.
- Individual applications that use system specific passwords, rather than University Domain passwords, should be set and managed in accordance with the specific system requirements and meet the password strength criteria established within the respective system(s).
- In all cases, every effort should be made to create/use strong passwords that consist of a variety of upper and lower-case letters; numbers; and special characters that are not easily guessed (names, important dates, etc.).

- If a user's password is compromised for any reason the user should immediately change the password and report the incident to the Office of Information Technology Help Desk (336-841-HELP or helpdesk@highpoint.edu).

## Administrator Passwords

- Must be at least 12 characters long, and passphrases are strongly encouraged.
- Must meet complexity requirements of at least one number, at least one lowercase letter, at least one uppercase letter, and at least one special character.
- Should be changed quarterly or anytime staff/position turnover would result in an unauthorized user knowing an administrative password.
- The same password should not be used twice in a year.
- Should be documented and stored in a secure location for Management access in the event of an emergency.