

Password Policy

Information Technology

Purpose

The purpose of passwords is to defend against unauthorized access to Stetson University systems that could result in a compromise of personal or institutional data and to establish the identity of the person or service connecting to technology resources.

Scope

This policy covers all user accounts managed by Stetson University. This includes accounts managed through Active Directory, Banner, and all other systems and software.

Definitions

- **User Account:** Username and password used to identify and authenticate an identity typically used to access Stetson University resources.
- **Active Directory:** Authoritative directory used to store and manage user accounts.

Policy Statement

Part 1: Minimum Password/Passphrase

Stetson's default password policy for ALL systems is the following:

- Minimum of 15 characters using three of the four types of characters (uppercase letter, lowercase letter, numeric, and non-alphanumeric).
- Cannot include your first name, last name, or username.
- Cannot reuse one of your previous three passwords.
- Passwords must be changed every 180 days.

It is a best practice to create a passphrase that is a complete sentence (e.g., *This is a strong passphrase.*). A password is typically much harder to remember because it is typically ambiguous (e.g., *c0mpl3xP@ssword*).

Part 2: Additional Requirements

Passphrase Protection

- Passphrase should not be kept or transmitted in mediums that are easily compromised and not considered safe (i.e. written on paper, post-it notes, text messages, or email).
- Your personal passphrase should be kept confidential and never shared with others, including supervisors, coworkers, IT staff members, contractors, or anyone else.
- All systems and software which require a login must at a minimum use HTTPS to encrypt communication and encrypt the authentication verification traffic (i.e., LDAPS). Passphrase information should never be transmitted in any form without some type of encryption.

- Unless approved by IT, no software or systems operated, owned, or contracted by Stetson University should store passwords.

Passphrase Change

If you need to change your passphrase or you have forgotten your passphrase, you can visit <https://my.stetson.edu/pwdwizard/> to change or reset your password.

Questions

If you have questions or concerns regarding this policy or other Information Technology Security Policies, please contact the Office of Information Technology via phone: 386-822-7045, or email: support@stetson.edu.