Password Standard

Contents

Revision History

Standard	Effective Date	Email	Version	Contact	Phone
OIT-PS		strevena@csustan.edu	1.0	Stan Trevena	209.667.3137

Executive Summary

Passwords are the first line of defense for the computers, communications systems, and information security at Stanislaus State. It is the individuals' responsibility to maintain the security of their password while maintaining a certain level of complexity within that password as not to allow for breeches of that account. Usernames and password management is a significant part of our overall solution to improve security within Stanislaus State. The overall protection of the data assets must begin with the individual who has access to them. Password Standard defines the password requirements surrounding the management of access to information on Stanislaus State's computer and communication systems. The purpose of this standard is to define security protection controls that will help minimize the loss of confidentiality, integrity, and availability of Stanislaus State business information as it is stored, processed, and transmitted.

Introduction and Purpose

This standard defines the password requirements surrounding the management of access to information on Stanislaus State's computer and communication systems. The purpose of this standard is to define security protection controls that will help minimize the loss of confidentiality, integrity, and availability of Stanislaus State business information as it is stored, processed, and transmitted.

Scope

This standard applies to all Stanislaus State, Self-Funded, and Auxiliary ("campus") computer systems and facilities, with a target audience of Stanislaus State Office of Information Technology (OIT) employees and partners. This standard applies to all passwords which grant access to confidential Level 1 and Level 2 data. Wherever possible, this standard must be followed when configuring access control systems. Systems which cannot implement this policy must be approved and documented by the Information Security Officer.

Stanislaus State Password Standard

Length and Complexity

- Passwords must be between 12 and 127 characters.
- Passwords must contain three of the following four:
    - Upper Case Letter (A-Z)
    - Lower Case Letter (a-z)
    - Number (0 through 9)
    - Symbol that can be pronounced (no foreign characters)

Expiration

All passwords shall expire every 180 days.

Account Lockouts

Accounts shall be locked out after 5 consecutive failed login attempts. Lockout duration shall be 60 minutes, unlocked after 60 minutes (unless performed using reset server, see below).

Reusing Passwords

Passwords can be re-used following five password resets.

Password Reset Server

Users can register with the campus Password Reset Server at the following address:

http://reset.csustan.edu

By registering with this server, a user will be able to self-service either a password reset or unlock their account outside of the 60 minute autolock after failed password attempts. OIT strongly recommends that all Stanislaus State users register for this service. In the event that a user has not registered with this service, they can contact the Help Desk for assistance with password resets and unlocking their account (must be done in person in the Library with appropriate identification presented at time of reset).