Passwords Policy

Summary

Authentication, in the form of a user ID and password, is a means of protecting CSU information assets from misuse or compromise and is required to access all University owned computers.

Passwords are the front line of protection for network access. A poorly chosen password may result in the compromise of the entire CSU network.

Purpose

The purpose of this policy is to establish a standard for the creation of strong network passwords, the protection of those passwords, and for the frequency of change. This policy does not pertain to certain system applications passwords (ex. Banner, Peoplesoft), although the same principles apply.

Policy

The system prompts users to change their initial password upon first login and directs the user to the "CougarNet Reset Your Password" page.

The system forces periodic password changes. All users (students/faculty/staff) must change their password every 180 days since their last password reset.

Passwords must be a minimum of 10 characters and should adhere to these guidelines:

Passwords must contain characters from all four of the following types of characters:

- At least one lower case and one capital letter
- At least one numerical digit
- At least one of these special characters @ ! $ ~ ( ) ^ *
- At least 10 characters

- Passwords should be difficult to guess. Do not use derivatives of user-IDs, common character sequences (ABC123), a spouse's name, your birth date and the like.
- Password history is enabled and configured to disallow the same password used in the past three (3) times and (30) days.
- After 3 failed attempts to validate a user's identity there will occur a password reset portal lockout. The user will be required to contact the UITS Help Desk and follow the process to have the account unlocked.

Users must not reveal their password to another person, regardless of the circumstances. Users must not write down their passwords in easily discovered places.

Users must not store passwords in any type of communications programs such as electronic mail clients or Internet browsers.

Passwords should not be included in any part of an e-mail message.

Procedures and Responsibilities

Users must create their password using the CougarNet Reset Your Password Page at initial login.

Change – users are instructed to change their account password by using the CougarNet Reset Your Password Page.

UITS is responsible for meeting the USG IIT Handbook Section 5 (Information Security) password standards, any federal regulations and compliance requirements with respect to accepted secure authentication methods.

While UITS/InfoSec will make every effort in verifying the identity of any CSU user requesting a password reset, it is the user's responsibility to remember and safeguard their password.

If a user suspects that another individual has obtained their password, they must change their password and inform **InfoSec (abuse@columbusstate.edu) or** the UITS Help Desk **(helpdesk@columbusstate.edu)** immediately.

Related USG Policy

11.3 Information Security Policy

Last Update

4/16/2014

Responsible Authority

Chief Information Security Officer