Connecticut State
Colleges & Universities
Board of Regents for Higher Education

Information Technology
Standard

Remote Password Reset Standard

Identifier:	**Approved Date: March 13, 2020**
Revision Date: March 13, 2020	**Effective Date: March 13, 2020**
Approved by: Joe Tolisano	

Table of Contents

1. Introduction

A faculty member, staff member or student at one of the Connecticut State Colleges and Universities (CSCU) may be unable to reset a password using the automated, self-service password reset system because they do not have the required data, data is not available in the Information System to verify their identity or they are not authorized to use the self-service system. In these cases, the individual will need to contact their institution to have their password reset. The CSCU system needs to verify the individual's identity prior to the password reset and comply with the state and federal requirements on identity management.

2. Purpose

Provide a mechanism for faculty, staff and students to have their passwords reset via remote communication, verifying the individual's identity, while maintaining the security controls and meeting our federal and state regulatory requirements.

3. Scope

This applies to all CSCU constituent units.

4. Definitions

Identity Data

Identity data is any combination of information that will identify who you are. Typical identity data sets are first and last name, first initial and last name, first name and address.

DCL3 Data

DCL3 – Previously known as Class A Protected at the CSUS
Level 3 is protected confidential data, which comprises identity and financial data that, if improperly disclosed, could be used for identity theft or to cause financial harm to an individual or the CSCU System. Security at this level is very high (highest possible).

Examples of DCL3 data are:

- Social Security number & Identity Data
- Bank account or debit card information and Identity Data
- Credit card number & cardholder information
- Student Loan Data

DCL3 data must be protected from disclosure and maleficence.

DCL2 Data

DCL2 – Previously known as Class A at the CSUS
Level 2 is restricted data that is available for disclosure, and may be disclosed under certain circumstances e.g. FOIA, legal request, etc. Such information is restricted due to federal and state law, ethical and privacy considerations.

An example of such restrictions would be the FERPA guidelines that govern publication and disclosure of student information. Security at this level is high.

Examples of DCL2 data are:

- Mother's maiden name
- Academic records
- Employee Medical Records

Red Flag Rules

In 2003, the U.S. Congress enacted the Fair and Accurate Credit Transaction Act of 2003 (FACT Act) which required the Federal Trade Commission (FTC) to issue regulations requiring "creditors" to adopt policies and procedures to prevent identify theft.

In 2007, the Federal Trade Commission (FTC) issued a regulation known as the Red Flag Rule. The rule requires "financial institutions" and "creditors" holding "covered accounts" to develop and implement a written identity theft prevention program designed to identify, detect and respond to "Red Flags," patterns, practices or specific activities that indicate the possible existence of identity theft.

Information Security User Education and Awareness Training

A CSCU Information Security User Education and Awareness Training program that meets the minimum training requirements for access to DCL3 data.

CSCU Identity Management and Red Flags Training

The CSCU course on Identify Management, Information Security and the identification of Red Flags for possible identity theft.

Assurance Function

Assurance is the responsibility of the system owner and is the process the system owner uses to verify that both technical and administrative controls are functioning correctly.

5. Roles and Responsibilities

CSCU Employee - CSCU employees or authorized vendor with a minimum of DCL2 data access.

Student – Student in the CSCU system

Faculty – Faculty in the CSCU system

Staff – Staff in the CSCU system

6. Standards

6.1. Training and Access Requirements

- Only **CSCU employees** who have DCL3 data access with the appropriate training will be granted access to change passwords for faculty and staff.
- Only **CSCU employees** who have DCL2 data access with the appropriate training will be granted access to change passwords for students.
- All CSCU employees with access to change account passwords remotely will need to have attended an Information Security User Education and Awareness Training class that meets the CSCU training standard.

6.2. Community College Remote Password Reset Process

- The authorized CSCU employee verifies the individual's identity by verbally requesting the first and last name of the individual, the CSCU faculty/staff/student identifier, e.g. CCC – NetID, and last four digits of the SSN with at least 1 of the following identification elements comparing it to the data in the verification system (e.g. Banner).
    - Date of Birth
    - Address on file
    - Telephone number on file

  If the student record in Banner does not display an SSN, then the authorized CSCU employee verifies the individual's identity by verbally requesting the first and last name of the individual, the CSCU faculty/staff/student identifier (e.g. CCC – NetID) and all 3 of the following identification elements comparing it to the data in the verification system (e.g. Banner).
    - Date of Birth
    - Address on file
    - Telephone number on file
- The password will be reset to a random password that is verbally communicated.
- The following minimum information must be logged by the reset process: who performed the reset, Banner ID of individual whose password was reset, Date & Time reset occurred.
- After a password reset, the individual will be required to change their password immediately upon a successful login or access to system resources will be denied.

- Security questions and answers will be cleared and the individual will be required to establish a new security question and answer immediately upon a successful login or access to system resources will be denied.
- Any Red Flags during the password reset will stop the process. For the password to be reset over the phone the individual needs to be transferred to a staff member with full Banner Access who can verify the complete SSN and any additional information required under Red Flags.

6.3. CSU and COSC Remote Password Reset Process

- The authorized CSCU employee verifies the individual's identity by verbally requesting the first and last name of the individual, the CSCU faculty/staff/student identifier, e.g. CCSU – BlueNet ID, SCSU - Hoot Loot ID Card with at least 2 of the following identification elements comparing it to the data in the verification system (e.g. Banner).
  - Last four of SSN
  - Date of Birth
  - Address on file
  - Telephone number on file
- The password will be reset to a random password that is verbally communicated.
- The following minimum information must be logged by the reset process: who performed the reset, Banner ID of individual whose password was reset, Date & Time reset occurred.
- After a password reset, the individual will be required to change their password immediately upon a successful login or access to system resources will be denied.
- Security questions and answers will be cleared and the individual will be required to establish a new security question and answer immediately upon a successful login or access to system resources will be denied.
- Any Red Flags during the password reset will stop the process. For the password to be reset over the phone the individual needs to be transferred to a staff member with full Banner Access who can verify the complete SSN and any additional information required under Red Flags.

7. Control Metrics

Quarterly reports will be run to determine the number of passwords resets performed remotely, including the number unable to be reset during the Remote Password Reset Process.

A report on Red Flag events during each quarter will also be included.

8. Control Tests

Quarterly, an assurance function will attempt 5 remote password resets using Test Banner Accounts. Any deviations from the Student Remote Password Reset Standard will be documented and reported to management.

9. Exceptions

To request an exception, please submit the Information Security Exception request to SecProg@ct.edu

The requestor and BOR Information Security Program Office will define the approved alternative configuration if different than the original proposal of the requestor.

The exception process is NOT an alternative to the Change Control Management process.

10. Related Publications

Related Policies

- BOR Information Security Policy

Related Procedures

- Requesting or Revoking Access to the GWANTID Form
- User Guide for the GWANTID form

Web Sites

- Support Services Website

11. Revision History

Previous versions of this standard

- September 16, 2014

History of Changes

- None

Standards superseded by this standard

- None