CCC Data Users Procedures

	Scope: CCC
Revision Date: 9/1/2016	**Effective Date: 3/1/2015**
Approver: Information Security Program Office	

Table of Contents

1. Introduction

As outlined in the Information Security Education and Awareness Training Standard (IT-STND-002) the Information Security Education and Awareness Program is required for all Connecticut State Colleges and Universities (CSCU) Data Users who have access to DCL3 data. The primary component of the Information Security Education Program is:

1. Annual Comprehensive Training; SANS Securing the Human training, for all staff who have been identified as having access to DCL3 data, as well as staff who have transferred and now have access to DCL3 data.

2. End User Operational Procedures

2.1 Complete Comprehensive training

All CCC Data Users with access to DCL3 data must complete the comprehensive training.

All newly hired staff who have been identified as having access to the DCL3 data or staff that have transferred and now have access to DCL3 data, must complete the required comprehensive training within 2 weeks of hire**.**

Comprehensive Program: SANS**,** Securing the Human contains multiple video modules that range 2-5 minutes each.

1. Log into the SANS ACLP (Advanced Cybersecurity Learning Platform) with the credentials you received via email. If you did not receive credentials, or have forgotten them, please contact your Data Manager.
2. Complete the modules available to you. You do not need to complete the modules all at once; however, you must complete the modules by the due date or (within two weeks of your date of hire).

2.2 Save and maintain training certificate

All employees with access to DCL3 data are required to maintain their training completion certificates from SANS Securing the Human training. These certificates are available on the dashboard page after you complete the training.

It is your responsibility to maintain these documents in order to report the results to your Data Steward. These completion certificates are valid at all CSCU institutions. A SANS completion certificate from another CT state agency will also be accepted as proof that you have completed the training.

Note: Student Employees must forward their completion certificates to their Data Steward.

Certificate Sample:


SANS

Certificate of Completion

[redacted]

has successfully completed

2016 Information Security Awareness Interactive Modules

on
9/1/2016

Compliance Checklist

- ☐ Complete Training
- ☐ Document Training Compliance

Report History

- ☐ Comprehensive training complete
- ☐ Ongoing - New Hires complete Training

Definitions

Data Domain

Data belongs to specific functional areas, also referred to as a data domain

Examples of Data Domains are:

- Academic Records
- Admissions
- Development (Fundraising)
- Financial Aid
- Human Resources
- Information Technology
- Institutional Research
- Student Advising & Counseling

Data Steward

A Data Steward has planning and policy responsibilities for data within a specific functional area(s) or data domain. Data Stewards have responsibility for understanding, protecting and granting access to CCC data.

Data Manager

A Data Manager has day-to-day responsibilities for data management within a specific functional area(s) or data domain. Data Managers have responsibility for understanding, protecting and managing access to CCC data.

Data User

A data user has operational requirements to access data and use data in performance of his/her assigned duties.

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 Records

DCL1 Data

DCL1 – Previously known as Class B at the CSUS
Level 1 is internal data that has not been approved for general circulation outside the CSCU system where its disclosure would inconvenience the CSCU system, but is unlikely to result in financial loss or serious damage to credibility. Security at this level is controlled but normal.

Examples of DCL1 data are:

- Internal memos
- Minutes of meetings
- Internal project reports

DCL0 Data

DCL0 – Previously known as Class C at the CSUS
Level 0 is public data that has been explicitly approved for distribution to the public. Disclosure of public data requires no authorization and may be freely disseminated without potential harm to the CSCU system. Security at this level is minimal.

Examples of DCL0 data are:

- Advertising
- Public Directory Information
- Press Releases
- Job postings

SANS Securing the Human

SANS is online training that focuses on the individual and what they can do to help secure their organization and themselves.

Information Security Program

An information security program is the comprehensive safe-guarding of an organization's data from unauthorized access or modification to ensure its availability, confidentiality, and integrity