CCC Data Management Procedures – DCL3 Data Access

	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 Data Management Standard (IT-STND-001) and the Information Security Education and Awareness Training Standard (IT-STND-002) all Data Stewards must maintain a list of Data Domain users, their level of data access and based upon that access the completion of the required Information Security Education and Awareness Program trainings. All Connecticut State Colleges and Universities (CSCU) Data Users who have access to DCL3 data must complete the Information Security Education and Awareness Training Program annually. It is the Data Steward's responsibility to keep data user inventory and verify and report that users have complied with the awareness training requirements.

2. Data Management Reporting Process Overview

2.1. The Data Stewards/Data Managers will complete the Data Management Reports for the current reporting year and submit them to their Data Coordinator. (The Data Management Report inventories all Data Users within the Data Steward's Domain, their access level to data, and if they have met the training requirements of the program.)

2.2. Data Coordinators will compile the Data Management reports from all **Data Stewards**.

2.3. The Data Coordinators will submit the final compiled Data Management Report to the ISPO on or before **November 1st of the reporting year.**

3. Data Management Training Process Overview

3.1. The ISPO will announce to the Data Coordinators and **Data Stewards** when the Information Security Awareness Program will be made available.

3.2. The Data Stewards will inform their Data Managers/DCL3 Data users of the training requirement and deadlines.

3.3. DCL3 Data Users will complete the training and report results to the **Data Stewards/Data Managers.**

4. Data Management Procedures

4.1. Data Management Documentation

Data Stewards must maintain and update the record of all Data Users in their Data Domain with access to DCL2 and DCL3 data using the provided Excel spreadsheets, (Data Coordinators will provide the Data Stewards with these spreadsheets.) The records must include the level of data the Data User has access to (e.g. DCL3 Electronic Data/DCL3 Paper data or DCL2). Other information that is needed; Data User's user name, Net ID, email, phone number and date the security awareness training was completed.

The report is not only used to maintain an up-to-date record of Data Users and their access level, it is also used as the report to be submitted for training completion compliance.

Note: Access to DCL3 data can mean the user has access to electronic information or have access to physical documents and is reported separately. Annual training is required for anyone with access to both and includes but is not limited to staff, faculty, and student workers.

All **new** CSCU staff, who will have access to DCL3 data, must complete the required training within 2 weeks of hire. Any employee who has been on leave should complete the required training within 2 weeks of returning to work. Data for employees who have left CSCU service will be maintained in accordance with record retention rules.

Student workers or non-staff employees that also have access to DCL3 data must also be reported and are also required to complete training.

4.2. Ensure that DCL3 Data users complete the required yearly Information Security Awareness Program

4.2.1. All DCL3 Data Users must take the comprehensive SANS video training, Securing the Human which has multiple video modules that range 2-5 minutes each.

4.3. Requesting or Updating SANS Training Accounts

Data Stewards will use the SANSAccountRequestSpreadsheet.xlsx form to request access to the SANS Securing the Human accounts. Account creation may take up to 2 business days to be processed. When access is granted, an email is sent to the email address provided in the request. For students, use their Office 365 email address; for staff members, use their official institution email address (i.e. do not request access for personal email addresses). Send the completed form from your institution email (i.e. do not send from a personal email account) to the CSCU IT Support Center (ServiceDesk@ct.edu).

If an employee's information has changed (i.e. name change due to marriage, different department, email or phone number), then please use the following Change Form.

4.4. Report Compliance

Data Stewards for the CCC's are required to report Data Domain Users Access and training completion for the reporting year and any new employee training compliance by **November 1st of the reporting year**.

The reports must include all Data Users and their compliance/non-compliance with the Information Security Education and Awareness Training Program. The report will be used as the completed Data Management Report for your Data Domain for that year and needs to be given to your Data Coordinator.

4.5. Distribution List Maintenance

Data Steward and Data Manager Distribution Lists have been created for each of the Community Colleges. It is the responsibility of the IT Deans/Directors to populate the distribution lists and maintain them.

4.6. Data Role Updates

In the event that there is a change to a Data Steward or Data Manager's role, or a Data Domain is modified, open a support ticket with the CSCU IT Support Center (ServiceDesk@ct.edu) with the changes.

5. Compliance Checklist

- ☐ Identify Data Users and classify access level
- ☐ Document Training Compliance

6. Report History

☐	11/1/2016	-	2016 compliance report submitted
☐	11/1/2015	-	2015 compliance report submitted
☐	2/6/2015	-	2014 compliance report submitted
☐	10/26/2014	-	Data Domain Report due

7. Forms

SANS Account Request Spreadsheet

Change Form

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.