CCC Data Coordinator Annual Reporting Procedures

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

Table of Contents

1. Introduction

As directed by 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 users have complied with the awareness training requirements.

Data Coordinators are responsible for communicating, compiling and submitting the annual, Data Management Report including the Information Security Education and Awareness Training results provided by the Data Stewards.

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 Reporting Procedures

4.1. Data Domain Report

Data Coordinators must coordinate and consolidate the Data Domain Report record of all Data Domains, Data Stewards and Data Managers. Updates and changes to the report need to be emailed to the Information Security Program Office (ISPO) at secprog@ct.edu.

4.2. Data Management Report

Data Coordinators must coordinate and consolidate the 2016 Data Management Reports. These reports 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 on the form; Data User's user name, Net ID, email, phone number and date the security awareness training was completed.

The Data Management Coordinator is responsible for compiling the reports and sending them to the Information Security Program Office (ISPO) at secprog@ct.edu by **November 1, 2016.**

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** employees or employees who have changed job functions who will have access to DCL3 Data in their new position, are required to complete the SANS, Securing the Human Training within two weeks of employment. 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.

4.3. Distribution List Maintenance

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

4.4. 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 BOR IT Support Center (ServiceDesk@ct.edu) with the changes.

5. Compliance Checklist

- ☐ Reporting Year 2016 Data Management Report submitted

6. Report History

- ☐ 11/1/2016 – Report due — Reporting Year 2016 Data Management
- ☐ 11/1/2015 - Report due — Reporting Year 2015 Data Management
- ☐ 2/6/2015 - Report due — Reporting Year 2014 Data Management
- ☐ 10/26/2014 - due — Reporting Year 2014 Data Domain report

7. Forms

Blank Data Management Report

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 ConnSCU 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 ConnSCU system where its disclosure would inconvenience the ConnSCU 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 ConnSCU 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.