Connecticut State Colleges & Universities
Board of Regents for Higher Education

Information Technology

Standard

Information Security Education and Awareness Training

Identifier: IT-STND-002	
Revision Date: 9/1/2016	**Effective Date: 3/1/2015**
Approved by: BOR CIO	**Approved on date: 10/17/2014**

Table of Contents

1. Introduction

The CSCU system, based on our educational activities, needs to collect and process Personal Identifiable Information (PII) and academic data of our constituents. We are required by law to provide appropriate training to anyone who has access to DCL3 data on an annual basis and training on a regular basis is highly recommended, for users with PII and academic data access.

2. Purpose

The Information Security Education and Awareness Training standard specifies the minimum requirements for training based on the user's data access. The standard also specifies the required record keeping and reporting requirements for Data Stewards and Data Coordinator.

3. Scope

The standard applies to all CSCU constituent units.

4. Definitions

DCL3 Data

DCL3 – Previously known as Class A Protected at the CSUS
DCL3 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). A breach of DCL3 data requires notification to users.

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
DCL2 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. A breach of DCL2 data does not require notification to users.

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

Information Security User Education and Awareness Training

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

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.

Reporting Cycle

The reporting cycle ends each year on November 1st when the Security Program report is due to the system office. The system office reports the findings from the reporting cycle by November 15th, per the BOR Information Security Program Resolution.

5. Roles and Responsibilities

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 CSCU 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 CSCU data.

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

Data Management Coordinator – The Data Management Coordinator is responsible for communicating and reporting Information Security Education and Awareness Program initiatives.

6. Standards

6.1 Information Security Education and Awareness Program

The CSCU Information Security Education and Awareness Program is a comprehensive program with the following program components.

- An on-line information security training program comprised of modules. The modules required to be taken are based on the user's level of data access. Users with DCL3 data access will require a more comprehensive program than users with DCL2 data access.

- Mandatory annual training for users with DCL3 data access.
- Voluntary annual training for users with DCL2 data access.
- On-going user education initiatives to support the training. E.g. posters, e-mail communication, brown bag seminars, etc.
- Verification program to ensure users are following the Information Security Education and Awareness Program. E.g. targeted phishing, targeted social engineering attack, etc.

6.2 College/University Program Coordinator

Each college/university President will identify a Data Management Coordinator who will be responsible for the following:

- Communicating and providing resources to campus staff on the Information Security Education Awareness Training program.
- Acting as the point person for communication with the Information Security Program Office.
- Compiling and submitting the Information Security Education and Awareness Training Program annual report.

6.3 Information Security Education and Awareness Program for Users with DCL3 Data Access

All CSCU employees with potential access to DCL3 data are required to complete the Information Security Education and Awareness Training Program annually.

The 2016 training program consists of the following SANS Securing the Human modules:

- Social Engineering, E-mail and Messaging, Browsing, Social Networks, Mobile Device Security, Passwords, Encryption, Data Security and Data Destruction, Working Remotely, Insider Threat, Physical Security, Hacked, Advanced Persistent Threat, Cloud Services, PCI DSS, Personal Identifiable Information (PII), Federal Tax, GLBA, Red Flags Rule, Data Retention, Federal Personal Identifiable Information (PII), and Privacy Security.

Any new employee with potential access to DCL3 data is required to take the Information Security Training within 2 weeks of employment.

Attendance records for participation in the training programs components need to be maintained by the Data Steward within the Data Management Report spreadsheet and contain at a minimum, the following information:

- State Employee ID, User Name, e-mail, phone, DCL3 Access, DCL2 Access, DCL3 Training Complete, Date of DCL3 Training, Active Employee, Data of Hire, Last Date of Employment.

Note – Users who transfer departments with the same or lower level of data access may have their records transferred to the new department. Users who have higher data access will need to take the appropriate training within two weeks of transfer.

6.4 Information Security Education and Awareness Program for Users with DCL2 Data Access

It is highly recommended that all CSCU employees with potential access to DCL2 data complete the annual Information Security Education and Awareness Training Program.

The training program for DCL2 users should cover, at a minimum, the following topic areas:

- Social Engineering, E-mail and Messaging, Browsing, Social Networks, Mobile Device Security, Passwords, Encryption, Data Security and Data Destruction, Working Remotely, Insider Threat, Physical Security, Hacked, Advanced Persistent Threat, Cloud Services, PCI DSS, Personal Identifiable Information (PII), Federal Tax, GLBA, Red Flags Rule, Data Retention, Federal Personal Identifiable Information (PII), and Privacy Security.

It is recommended that any new employee with access to DCL 2 data take, the information security training within 2 weeks of employment.

Attendance records for participation in the training programs components need to be maintained by the Data Steward within the Data Management Report spreadsheet and contain at a minimum, the following information:

- State Employee ID, User Name, e-mail, phone, DCL3 Access, DCL2 Access, DCL3 Training Complete, Date of DCL3 Training, Active Employee, Data of Hire, Last Date of Employment.

Note – Users who transfer departments with the same or lower level of data access may have their records transferred to the new department. Users who have higher data access will need to take the appropriate training within two weeks of transfer.

7. Reporting Requirements

Annually by November 1st the Data Management Coordinator will submit to the Information Security Program Office a consolidate report of training done during the past reporting cycle.

8. Control Metrics

- Participation rate for online training courses - percentage of staff completing security training (by business unit)
- Average scores of online tests, compared to baseline (previous tests, industry data if available, etc.) by business unit
- Average scores of periodic tests (e.g. click rates for test phishing emails) by business unit
- Individual scores on skill assessment tests for individual mission critical roles by business unit

9. Control Tests

Quarterly, an assurance function will conduct a security test (targeted phishing, social engineering, etc.). They will develop an appropriate random sample and report on the test.

10. 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.

11. Related Publications

Related Policies

- BOR-Information Security Policy

Related Procedures

- Support Services Procedure Website
- [Link to Procedures page for Requesting Access to Password Reset Form]

Web Sites

- Support Services Website

12. Revision History

Previous versions of this standard

- Revision 1 - 8/1/2015
- Revision 2 – 9/1/2016

History of Changes

- 8/1/2015
  - Clarification to the timeline with the reporting cycle ending on Nov. 1st.
- 9/1/2016
  - Adjustments made to reflect changes in SANS Securing the Human course listings.

- Standards superseded by this standard
  - 2007 CSUS Information Security Standards V 1.0
    - Section 4.7 Security Awareness, Training, and Education