Policy:

CSCU will: (i) ensure that managers and users of information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of CSCU information systems; and (ii) ensure that CSCU personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.

Scope:

1. Institutional Units of the Connecticut State College and University System including the Connecticut Board of Regents System Office.

2. All Connecticut State College and University institutional units' information systems.

Procedure:

1. Awareness and Training Process

1.1 The ISPO will announce to the Data Coordinators and Data Stewards when the Information Security Awareness Training will be made available.

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

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

2. Awareness and Training Reporting Process

2.1 The Data Stewards/Data Managers will complete the Data Management Reports for the reporting year, July 1 – June 30 and submit them to their Data Coordinator. For 2017 we are collecting the training completion of all new DCL3 data users throughout the reporting year, July 1, 2016 – June 30, 2017. The most current Data Management reports should be used.

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 1, 2018.

3. Data Management Report

3.1 Data Management Report

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.

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.

3.2 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.

3.3 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, make the changes in your report and send an updated copy to ISPO.

Roles and Responsibilities

1. **Data Management Coordinators**
    a. **Act as liaisons to the Informaiton Security Program Office**
2. **Data Users**
    a. **Use DCL3 data as part of their required work responsibilities**
3. **Data Managers**
    a. **Manage DCL3 data users**
4. **Data Stewards**
    a. **DCL3 data owners responsible for:**
        i. **granting access to the DCL3 data within their Data Domain.**

ii. **ensuring that the DCL3 data users within their data domain are completing the required Awareness and Training Program.**

iii. **completing the annual Data Management report requirements.**

Definitions

Refer to the Glossary of Terms located on the website.

References

CT Board of Regents for Higher Education Resolution; Concerning the Design, Implementation Operational Management and Assurance/Compliance of the Information Security Program for the Board of Regents of Higher Education, October 17, 2013.

IT-003, Information Security Policy, March 2015.

NIST 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013.

NIST 800-171 Rev. 1, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, December 2016.

General Records Retention Schedules for State Agencies, S6: Information Systems Records, Connecticut State Library, Office of the Public Records Administrator, Item S6-100, December 2010.

Revision History

Date	Change	Revision	Signature