Data Management

Identifier: IT-STND-001	
Revision Date: 8/1/2015	**Effective Date: 03/1/2015**
Approved by: CSCU CIO	**Approved on date: 10/17/2014**

Table of Contents

1. Introduction

Data Management addresses the activities of capturing, storing, protecting, using, disseminating, and destroying data. Good data management requires a governance context within which to operate; and data management policies, standards and procedures provide guidance for the routine handling and protection of institutional data and media containing that data. Data management practices should improve efficiencies, reduce risks associated with handling data, and ensure institutional compliance with applicable regulations, such as State of CT record retention schedules. Good data management also minimizes misuse, misinterpretation, or unnecessary restrictions of access to institutional data.

Data Classification is the foundation for making decisions about data. Classification determines which security, storage, backup and other controls to implement. For example, public data needs less security than data that if compromised, could cause identity theft or financial fraud.

2. Purpose

This policy describes the strategy and responsibility for managing CSCU data at the College, Universities and System Office.

3. Scope

The standard applies to all CSCU constituent units.

4. Definitions

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 management roles and responsibilities:

- Data Steward
- Data Manager
- Data User
- Data Management Coordinator
- Records Management Liaison Officer (RMLO)

Data management roles are not exclusive and a single user could occupy all roles. Responsibility for ensuring data is managed appropriately for a functional area is the responsibility of the Data

Steward. The Data Steward can optionally assign daily operational functions to a Data Manager or perform the activities themselves.

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. More specifically he/she:

- Authorizes Data Users for their data domain(s)
- Verifies CSCU polices are being adhered to by the practices used in their functional area(s) for managing and protecting 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. More specifically he/she:

- Consults with data users about the meaning and interpretation of data elements
- Defines data (name, location, aliases, classification, metadata)
- Produces data (capture, generate, normalize, renew, label, document)
- Assures complete, accurate, valid, and timely data collection
- Provides accessible, meaningful, and timely machine-readable institutional data for CSCU use
- Mentors and trains staff
- Resolves problems associated with data
- Evaluates security, backup / recovery, and disaster recovery procedures
- Verifies data storage requirements for shared data

Data User

A data user has operational requirements to access data and use data in performance of his/her assigned duties. More specifically he/she:

- Retrieves, assembles and distributes data to other authorized data users
- Protects data with encryption techniques
- Monitors data usage
- Corrects data

Data Management Coordinator

- Coordinates and compiles data reporting for the college, university, or system office
- Coordinates training for Data Stewards, Data Managers and Data Users

Records Management Liaison Officer (RMLO)

The Records Management Liaison Officer is responsible coordinate with the State Librarian to carry out the provisions Connecticut General Statutes (CGS) Sec. 11-8a (f). The RMLO has primary responsibility for:

- Training of staff on records management requirements
- Coordinating with the state library on records destruction

***Note** - We recommend the role of RMLO is combined with the role of Data Steward and the institution assigns a primary RMLO of the unit and a secondary RMLO for each Data Domain.*

6. Data Classification

Data Classification is the process of grouping data elements together by risk level. CSCU has identified four Data Classification Levels, (DCL), from DCL0 to DCL3. Appropriate security controls will be applied to each classification level. Increasingly restrictive data management and security practices are required for each level, with DCL0 requiring limited protection to DCL3 requiring the most protection.

Data Classification Levels

Data Classification Level (DCL)	Description	Examples
DCL3	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 CSCU. Security at this level is very high (highest required).	**Identity Data with:** • Social Security number • Bank account or debit card information • Credit card number & cardholder information • Student Loan Data
DCL2	DCL2 is restricted data that is available for disclosure, but only under strictly controlled circumstances. Such information must typically be restricted due to proprietary, ethical or privacy considerations. An example of such restrictions is the FERPA guidelines that govern publication and disclosure of student information. Security at this level is high.	**Identity Data with:** • Birth date • Mother's maiden name • Academic records (e.g. Grades, Test scores, Courses taken, etc.) • Student Records (e.g. Advising records, Disciplinary actions) • Employee Records
DCL1	DCL1 is internal data that has not been approved for general circulation outside CSCU where its disclosure would inconvenience CSCU, but is unlikely to result in financial loss or serious damage to credibility. Security at this level is controlled but normal.	• Internal memos • Minutes of meetings • Internal project reports

Data Classification Level (DCL)	Description	Examples
DCL0	DCL0 is public data that is not classified as DCL1 through DCL3 and is approved for distribution to the public. Disclosure of public data requires no authorization and may be freely disseminated without potential harm to CSCU. Any data that does not have a classification listed above can be considered DCL0. Security at this level is minimal.	• Advertising • Public Directory Information • Press Releases • Job postings • Campus Maps

7. Data Domains

- All CSCU data will be viewed as belonging to or originating from a specific functional area, also referred to as a Data Domain.
- Each Data Domain will have a Data Steward, a Data Manager and Data Users.
- The originating Data Domain is considered the authoritative source for that data.
- Each College, University and System Office need to identify a Data Domain structure that works within their organizational structure: Following are examples of possible Data Domains.
  - Academic Records
  - Admissions
  - Bursars
  - Business Services
  - Development (Fundraising)
  - Facilities
  - Finance
  - Financial Aid
  - Human Resources
  - Information Technology
  - Institutional Research
  - President's Office
  - Registrars
  - Student Services
  - Student Advising & Counseling

8. Data Access Responsibilities

Responsibilities for all users with access to CSCU data:

- Protect CSCU data from unauthorized disclosure, corruption, or loss.
- Use CSCU data for legitimate and authorized purposes.
- Access only CSCU data for which you have been given authorized access.
- Employees will need to attend a Data Management course as part of a comprehensive Information Security awareness program.

9. Standards

9.1 Data Management Coordinator

Each CSCU President will define for their constituent unit a Data Management Coordinator. The Data Management Coordinator is responsible for the following:

- Coordinating and compiling data reports for the college, university, or system office
- Coordinating training for Data Stewards, Data Managers and Data Users

9.2 Data Domains at the Colleges, Universities and System Office

The CSCU President will define the constituent units' data domains for the institution. The institution can define the Data Domain structure that works with their organizational structure. For each Data Domain a corresponding Data Steward needs to be assigned. The Data Domain information for each constituent unit is maintained on the DataDomainReport.xlsx

9.3 Management of Data

Each Data Steward is responsible for the following with respect to their Data Domain:

- Designate a Data Manager(s) for the Data Domain. The Data Manager may be the Data Steward if the Data Domain only covers a small number of Data Users.
- Development of Data Domain operational procedures for appropriate handling and storage of data.
- Maintain an inventory of all Data Managers and Data Users for the Data Domain. The data inventory needs to contain the following information:
    - User name
    - User e-mail address
    - User phone
    - Role(s) – Data Steward, Data Manager, Data User
    - DCL3 Data Access – Yes/No
- Maintain and inventory of all data storage location(s) for the Data Domain. The data inventory needs to contain the following information:
    - Data Domain
    - Data Locations(s) – Inventory of all data storage locations – e.g. file shares, local drives, removable drives, backups, etc.
    - Data Access – Individual / Group, with list of users access
    - Data User/Manager assigned as primary user for group the location
    - Electronic storage area, Yes/No
    - DCL3 Data Location, Yes/No
    - For all DCL3 Data locations the following additional information needs to be maintained:
        - Data Application – e.g. Banner, Excel File, Paper Transcripts, Scanned Transcripts
    - Data Type – e.g. SSN, Driver's License/SSN, Bank Accounts, etc.
    - Data Encryption – Yes/ No – If yes, encryption used

- The inventories will be maintained in the following Excel spreadsheet or in a CSV formatted file. The Excel spreadsheet had a tab for each inventory type and a tab with the file format specification for the CSV file. Data Storage Location Report
- DCL3 Data Storage Verification
  - A Identity Finder Scan is performed on all electronic storage areas that are not designated to store DCL3 data
  - A log is maintained (electronically or manually) of the data verification that contains the following information:
    - Date of Scan
    - Location(s) scanned
    - DCL3 potential data found Yes/No
      - If yes, action taken – moved, false positive

9.4 Records Management

Each Data Steward has records management responsibilities for their data domain. The Records Management Liaison Officer (RMLO) for each institution is responsible for ensuring records are kept in compliance with State of Connecticut Record Retention Schedules and should coordinate with the institution's data stewards to ensure timely compliance. It is required that each institution identify an institution wide Records Management Liaison Officer (RMLO).

Records retention is based on the content of the message not the media in which it is communicated. Electronic messages, e.g. e-mail, texts, instant messages, etc. need to retain the Meta data along with message content. Any record that was required to be saved under records retention needs to go through the records destruction approval process before being deleted. Additional information on records management

State of CT Records Management Program
http://www.ctstatelibrary.org/public-records-programs/state-records-management-program

10. Reporting Requirements

Annually the Information Security Program Office is required to report to the Board of Regents on the CSCU security program. As part of the Program Office reporting the following reports for each constituent unit are due by Due by November 1st. The Data Management Coordinator is responsible for compiling the reports and sending them to the Information Security Program Office (ISPO) at secprog@ct.edu.

- List of Data Domains and assigned Data Stewards, - please submit in Excel form DataDomainReport.xlsx
- List of Data Domain users and training taken during the reporting cycle BLANKDataManagementReport.xlsx

11. Report Metrics

- Percentage of new staff, with DCL3 data access, who completed Information Security User Education Awareness program within the first two weeks of employment
- Average score of new staff taking Information Security User Education Awareness program
- Percentage of current staff, with DCL3 data access, who completed Information Security User Education Awareness refresher during the training window
- Average score of current staff taking Information Security User Education Awareness program

12. Control Metrics

- Percentage of new staff, with access to DCL3 data, who took the Information Security User Education Awareness program within the first two weeks of employment. - >95%
- Percentage of new staff, with access to DCL3 data, who took the Information Security User Education Awareness program with the first two months of employment. - 100%
- Percentage of current staff, with access to DCL3 data, who took the Information Security User Education Awareness program during the training window. - >95%
- Percentage of current staff, with access to DCL3 data, who took the Information Security User Education Awareness program during the fiscal year. - 100%.

13. Control Tests

- Semi-annually the Data Steward will randomly select 5% of the population (minimum three employees) and verify that user education training and data management has been completed.
- 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.

14. Exceptions

To request an exception, please submit the Information Security Exception request to SecProg@ct.edu

The requestor and CSCU 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.

15. Related Publications

Related Policies

- BOR-Information Security Policy

Related Standards and Procedures

- Link to Support Services Procedure Page

Web Sites

- Support Services Website

16. Revision History

Previous versions of this standard

- None

History of Changes

- Minor revisions to clarify the timeline as the reporting cycle ending on Nov. 1st.

Standards superseded by this standard

- 2007 CSUS Information Security Standards V 1.0
    - Section 3.4 Asset Classification
    - Section 6.2 Data Security
- 2011 CCC 4.1 Data Management Policy