DATA CLASSIFICATION STANDARD (DCS)

Objective

To implement a standard for Suffolk County Community College ("the College") that classifies data into one of the four (4) categories described herewith and defines the minimum security measures appropriate to safeguard that data/information.

Summary

Federal and state laws require certain organizations, including higher education institutions, to implement a DCS. The DCS is intended to compliment and supplement the College's current policies and procedures on data protection, data access, system administration, and information security. Compliance with the following standard does not ensure that data will be properly protected; instead the DCS should be integrated into a comprehensive information security plan.

All College data must be classified into one of the following four (4) categories:

Data Classification	Institutional Risk from Disclosure	Description	Examples
Category I: Regulated Private Data	High	Regulated data whose unauthorized access or loss could seriously or adversely affect the College, a partner, or the public. Security breaches of these data are subject to the New York State Information Security and Breach Notification Act and other federal, state, and industry rules and regulations. Credit card numbers, and how the college handles credit card transactions, are also subject to the Payment Card Industry Data Security Standard (PCI DSS).	• Social Security Number • Driver's License Number • State-issued Non-driver's ID Number • Bank/Financial Account Number • Credit/Debit Card Number • Electronic Protected Health Information • Passport Number • Trade Secrets
Category II: Protected Data	Medium	Regulated data subject to FERPA or other federal, state, or business regulation; any data specifically exempt from release/disclosure to the public by state or federal statute. This includes data exempt from disclosure in New York State's Freedom of Information Law (FOIL). FOIL exempts data that, if disclosed, would constitute an unwarranted invasion of personal privacy.	• College Network Access Credentials • FERPA Protected Information (Final Course Grades, Exam Questions and Answers, Student ID Numbers) • HR Employment Data • Law Enforcement Investigation Data • Judicial Proceedings Data (includes Student Disciplinary Action) • Public Safety Information • IT Infrastructure Data • Collective Bargaining/ Contract Negotiation Data • Protected Data Related to Research • College Intellectual Property • College Proprietary Data • External Non-Disclosure Agreement Data • Inter- or Intra-Agency Data which are not: statistical or factual tabulations; instructions to staff that may affect public; or final policies or determinations

Category III: Internal Use Data	Low to Medium	All other non-public data not included in Category I or II.	• College Financial Data • College Employee ID Number • Meeting Minutes • Administrative Process Data (about decisions that affect public) • Licensed Software • Other Non-Public Data
Category IV: Public Data	None	All public data.	• General Access Data (such as that found on unauthenticated portions of www.sunysuffolk.edu)

All data owners and users are required to implement appropriate technical security measures to protect the data consistent with the minimum security standards. Category I data has more stringent requirements than Categories II, III, and IV, but all systems need some degree of protection.

Data that is personal to a particular employee and generated by "incidental personal use" of College IT resources does *not* fall under the requirements for safeguarding confidential information. However, efforts must still be made to keep this information properly protected from unintentional and unwanted disclosure.

Applicability and Scope

This policy applies to all College community members, as well as to external vendors, contractors, guests, and visitors.

Definitions

1. **Category I – Regulated Private Data.** Regulated private data is classified using the definition of "private information" in the New York State Security and Breach Notification Act of 2005 – for example, bank account/credit card/debit card numbers, Social Security Numbers, state-issued drivers' license numbers, and state-issued non-drivers' identification numbers. Note that Category I data is exempt from disclosure/release under FOIL. The Breach Notification Act requires that the College must disclose any breach of the data to NY residents. The data elements that comprise the Category I data are reviewed regularly and subject to change.
2. **Category II – Protected Data.** Includes data not identified as Category I data, but data protected by state and federal regulations. This includes FERPA-protected student records and electronic records that are specifically exempted from disclosure by FOIL (http://www.dos.state.ny.us/coog/foil2.html). Such data must be appropriately protected to ensure that it is not disclosed in a FOIL request. FOIL excludes data that, if disclosed, would constitute an unwarranted invasion of personal privacy. The College currently identifies computer passwords and other computer access protection data (e.g., Network Access Credentials) in Category II.
3. **Category III – Internal Use Data.** Includes non-public data not included in Category I or Category II. Internal Use data also includes College ID numbers, licensed software, as well as College business records, intellectual property, and any non-public data that is releasable in accordance with FOIL.
4. **Category IV – Public Data**. General access data, such as that available on unauthenticated portions of the College website. Category IV data has no requirements for confidentiality.

Posted 20170303