# POLICY:
# DATA CLASSIFICATION

EFFECTIVE: SEPTEMBER 6, 2017

FACULTY ONLY: EFFECTIVE JANUARY 1, 2018

## 1.0 PURPOSE

The purpose of this policy is to define the data classification requirements for information assets in electronic format and to ensure that data is secured and handled according to its sensitivity and the impact that theft, corruption, loss or exposure would have on the institution.

This policy has been developed to assist, provide direction to and govern all entities of the New York Six Liberal Arts Consortium (NY6) regarding identification, classification and handling of information assets.

## 2.0 DEFINITIONS

*Data:* Information in a specific representation, usually as a sequence of symbols that have meaning.

*Data Asset:* Any entity that is comprised of data. The terms "information asset" and "data asset" are used interchangeably throughout this document.

*Source: Committee on National Security Systems Instruction No. 4009 (CNSSI-4009)*

## 3.0 SCOPE

The scope of this policy includes all information assets governed by the NY6. All personnel and third parties who have access to or utilize assets of the NY6 institutions, including data at rest, in transit or in process shall be subject to these requirements. This policy does not apply to:

- Personal information,
- Faculty Research, or
- Teaching materials.

## 4.0 POLICY

NY6 has established the following requirements regarding the classification of data to protect NY6 information:

### 4.1 DATA OWNERSHIP AND ACCOUNTABILITY

Data owners are identified as the individuals, roles or committees primarily responsible for information assets. These individuals are responsible for identifying the organization's information assets under their areas of supervision, and maintaining an accurate and complete inventory for data classification and handling purposes.

Data owners are accountable for ensuring that their information assets receive an initial classification upon creation and a re-classification whenever reasonable. Re-classification of an information asset should be performed by the asset owners whenever the asset is significantly modified. Data owners are also responsible for reporting deficiencies in security controls to management.

### 4.2 DATA CLASSIFICATION

Classification of data will be performed by the data asset owner based on the specific, finite criteria as identified in the Federal Information Processing Standard Publication 199 (FIPS-199) for confidentiality, integrity and availability. Refer to the Data Classification and Handling Procedure to determine how data should be classified. Data classifications will be defined as follows:

- *CONFIDENTIAL* - Information assets whose loss, corruption, or unauthorized disclosure would cause financial loss or would result in regulatory or government sanctions such as violations of federal or state laws or security breaches that result in the compromise of customer or associate private information. Common examples include but are not limited to student grades, banking and health information, credit card holder data, SSN's, faculty and staff personnel records, and information systems' authentication data.

- *SENSITIVE* - Information assets whose loss, corruption, or unauthorized disclosure would not seriously impair business functions but is otherwise private. Examples include financial statements, contracts, legal information and research data.

- *PUBLIC* - Information assets whose loss, corruption, or unauthorized disclosure would not impair business functions. Examples include sales and marketing strategies, web site content, building plans and promotional information, student directory information as prescribed by FERPA.

- *UNCLASSIFIED* - Information assets that have not yet been classified. All information assets default to this state prior to classification.
- *PROHIBITED* - Information assets whose creation, storage, processing or transmission are not permitted. Examples include information prohibited by law or contract, such as unlicensed software, copyrighted material and payment card information that cannot be stored in accordance with the Payment Card Industry Data Security Standard (PCI-DSS).

### 4.3 DATA HANDLING

Information assets shall be handled according to their prescribed classification, including access controls, labeling, retention policies and destruction methods. The specific methods must be described in an official Data Classification and Handling Procedure.

### 4.4 RE-CLASSIFICATION

A re-evaluation of classified data assets will be performed at least once per year by the responsible data owners. Re-classification of data assets should be considered whenever the data asset is modified, retired or destroyed.

### 4.5 CLASSIFICATION INHERITANCE

Assets, logical or physical, that "contain" a data asset may inherit classification from the data asset(s) contained therein. In these cases, the inherited classification shall be the highest classification of all contained data assets.

## 5.0 ENFORCEMENT

Users who violate this policy may be denied access to the institution's resources and may be subject to penalties and disciplinary action both within and outside of the institution. The institution may temporarily suspend or block access to an account, prior to the initiation or completion of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security or functionality of institution or other computing resources or to protect the institution from liability.

## 6.0 EXCEPTIONS

Exceptions to this policy must be approved in advance by the Chief Information Officer, at the request of the responsible data asset owner. Approved exceptions must be reviewed and re-approved annually.

## 7.0 REFERENCES

- Procedure – New York Six (NY6) – Data Classification and Handling
- Quick Reference – New York Six (NY6) – Data Classification and Handling
- Committee on National Security Systems Instruction No. 4009 (CNSSI-4009)

## 8.0 REVISION HISTORY

| Version | Date | Author | Revisions |
|---|---|---|---|
| **1.00** | 02-10-15 | GreyCastle Security | Original |
| **1.01** | 04-01-15 | GreyCastle Security | Union College Updates |
| **1.02** | 05-06-15 | GreyCastle Security | Union College Updates |
| **1.03** | 02-04-16 | GreyCastle Security | Union College Updates |
| **1.04** | 02-18-16 | GreyCastle Security | Union College Updates |
| **1.05** | 03-02-16 | GreyCastle Security | Union College Updates |
| **1.06** | 03-03-16 | GreyCastle Security | Union College Updates |
| **1.07** | 03-04-16 | GreyCastle Security | Union College Updates |
| **1.08** | 03-09-16 | GreyCastle Security | Union College Updates |
| **1.09** | 03-15-16 | GreyCastle Security | Union College Updates |
| **1.10** | 03-15-16 | GreyCastle Security | Union College Updates |
| **1.11** | 05-09-16 | GreyCastle Security | Union College Updates |
| **1.12** | 10-16-17 | Union College | Union College Updates |