PROCEDURE: DATA CLASSIFICATION AND HANDLING

EFFECTIVE: 09-19-2017

1.0 PURPOSE

Classification of data is a critical element of any mature information security program and fundamental to securing New York Six Liberal Arts Consortium (NY6) information assets. This procedure has been developed to assist, provide direction to and govern all entities of the organization regarding identification, classification and handling of information assets. The Campus expects all third party service providers to adhere to the institutions' security policies. If non-public information is to be accessed or shared with these third parties, they should be bound by contract to abide by these requirements.

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.

Personally Identifiable Information (PII) is defined as the first name or first initial and last name, in combination with any one or more of the following data elements:

- Government-Issued Identification Number
  - Social Security Number (SSN) / Taxpayer Identification Number (TIN) / National Identification Number (NIN) / Other similar national identification
  - Passport number
  - Permanent resident card

- Driver License (DL) Number

- Financial account number:
    - Payment card number (credit or debit)
    - Bank account number
    - Electronic Protected Health Information (ePHI)

Electronic Protected Health Information (ePHI): A combination of two or more data elements that uniquely identify an individual that would provide knowledge of medical information about the individual as defined by the Health Insurance Portability and Accountability Act (HIPAA).

File transfer protocol (FTP): A standard network protocol used for the transfer of computer files between a client and server on a computer network.

Instant Messaging: A type of chat offering real-time text transmission over the internet or other communication medium (e.g. cellular, Near-Field Communication (NFC), etc.).

Institution Financial Information: Information about the institution's finances, investments or investment strategies that are not public knowledge.

Payment Card Industry (PCI): Data associated with payment cards issued by the major payment brands (Visa, MasterCard, AMEX, Discover, etc.).

Payment Card Industry (PCI) Data or "Cardholder" Data: Account data associated with payment cards issued by the major payment brands (Visa, MasterCard, AMEX, Discover, etc.). It includes the Primary Account Number (PAN), expiration date and card verification code.

Intellectual Property (IP): Information about works, inventions or any other intellectual materials that give the institution a competitive advantage.

Confidentiality: Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

Integrity: Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity.

Availability: Ensuring timely and reliable access to and use of information.

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

3.0 ROLES AND RESPONSIBILITIES

- IT Security – Responsible for creating and managing many of the asset inventories used to store, process, transmit or provide access to electronic information. ITS is the custodian for this procedure.
- Chief Information Officer (CIO) – Responsible for monitoring the implementation of this procedure and reporting to senior management on any abnormal findings or exceptions.
- All Employees –
    - Responsible for classifying and marking all created or modified information, including any reproductions that are made (e.g. reports).
    - Responsible for handling all classified information (electronic or non-electronic) in accordance with Step 5 of Section 6.

4.0 DATA CLASSIFICATION LEVELS

Information assets shall be handled according to their prescribed classification, including access controls, labeling, retention policies and destruction methods, among others.

Information assets are assigned a classification level based on the appropriate audience for the information. If the information has been previously classified by regulatory, legal, contractual or institution directive, then that classification will take precedence. The classification level then guides the selection of protective measures to secure the information. All information assets are to be assigned one of the following three classification levels:

CLASSIFICATION		DATA CLASSIFICATION DESCRIPTION
CONFIDENTIAL	Definition	- Confidential information is highly-valuable, highly-sensitive institution information. The level of protection is generally dictated externally by legal and/or contractual requirements, but may also be generated internally as it relates to relevant confidential institutional information. -Confidential information must be limited to only authorized employees, contractors and business partners with a specific business need.

CLASSIFICATION		DATA CLASSIFICATION DESCRIPTION
	Potential Impact	**Significant damage** would occur if Confidential information were to become available to unauthorized parties either internal or external to Union. **The impact** will negatively affect Union's's compliance with regulatory requirements, damaging the instituion's reputation, and posing an identity theft risk.
SENSITIVE	Definition	- Sensitive information is highly-valuable, sensitive instituion information and the level of protection is dictated internally by Union. - Sensitive information is information originated or owned by Union, or entrusted to it by others. Sensitive information may be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the instituion's business interests.
	Potential Impact	**Moderate Damage** would occur if Sensitive information were to become available to unauthorized parties either internal or external to Union. **The impact** could include negatively affecting Union's reputation, violating contractual requirements, and exposing personal information about Union's employees or students.
PUBLIC	Definition	Public information is information that has been approved for release to the general public and is freely shareable both internally and externally.
	Potential Impact	**Minimal or no damage** would occur if Public information were to become available to parties either internal or external to Union. **The impact** would not be damaging to Union's reputation or a risk to instituion operations.

5.0 DATA CLASSIFICATION LABELING

Data classification labeling is the practice of marking an information system or document with its appropriate classification level based on the type of information it contains so that others know how to appropriately handle the information. There are several methods for labeling information assets.

- **Printed**: Information that can be printed (e.g., spreadsheets, files, reports, drawings, or handouts) should contain one of the following confidentiality symbols in the document footer on every printed page, or simply the words if the graphic is not technically feasible. The exception for labeling is with

marketing material, since marketing material is primarily developed for public release.

- **Displayed**: Restricted or Private information that is displayed or viewed (e.g., websites, presentations, etc.) must be labeled with its classification as part of the display.

CONFIDENTIAL	Access Limited to Authorized Personnel Only
SENSITIVE	Access Limited to Internal Use Only
PUBLIC	Public Release Authorized

GENERAL GUIDELINES

- Any information created or received by Union employees in the performance of the their job at Union is Private (Internal Use), by default, unless the information requires a higher classification or is approved for release to the general public.
- Treat information that is not assigned a specific classification level as "Private" at a minimum and use corresponding controls.
- When combining information with different sensitivity levels into a single application or database, assign the most restrictive classification to the combined asset. For example, if an application contains Private and Restricted information, the entire application is Restricted.
- Restricted and Private information must never be released to the general public but may be shared with third parties, such as government agencies, business partners or consultants, when there is a business need to do so and the appropriate security controls are in place according to the level of classification.
- You may not change the format or media of information if the new format or media you will be using does not have the same level of security controls in place. For example, you may not export restricted information from a secured database to an unprotected Microsoft Excel spreadsheet.

6.0 PROCEDURE

STEP 1 – IDENTIFY DATA ASSET

Identification of information assets involves creating an inventory of all information assets in the organization.

In order to facilitate the classification of information assets and allow for a more efficient application of controls, it may be desirable to group information assets together. It is important

to establish that the grouping of assets for classification is appropriate. A broad grouping may result in applying controls unnecessarily as the information asset must be classified at the highest level necessitated by its individual data elements. For example, if Human Resources decides to classify all of their personnel files as a single information asset and any one of those files contains a name and social security number, the entire grouping would need to be protected with the controls for a confidentiality of High.

A narrow grouping allows for more precise targeting of controls. However, as there are more information assets to classify, this increases the complexity of the classification and the management of controls. Using the previous example, classifying the multitude of personnel files (e.g., appointment letters, timecards, position classifications, holiday waivers) as individual information assets requires a different set of controls for each classification.

In the case of a system (e.g., database, data warehouse, application server), it may be easier to apply controls if the system is classified as a single entity. However, costs may be reduced by applying the controls to the individual elements (e.g., field, record, application). Therefore, it is important that the organization evaluate the difference between the two to identify the most appropriate solution when determining the grouping of information assets for classification.

Example:

Asset Name	Asset Owner	Confidentiality	Ingetrity	Availability	Classification
Student Grades					
Admission Data					
Annual Report					
Health Records					

STEP 2 – IDENTIFY DATA ASSET OWNER

It is important to place the responsibility for the classification and control of an information asset with an individual or role. This should be an individual in a managerial position. If multiple individuals are found to be "owners" of the same information asset, an individual owner should be designated by a higher level of management.

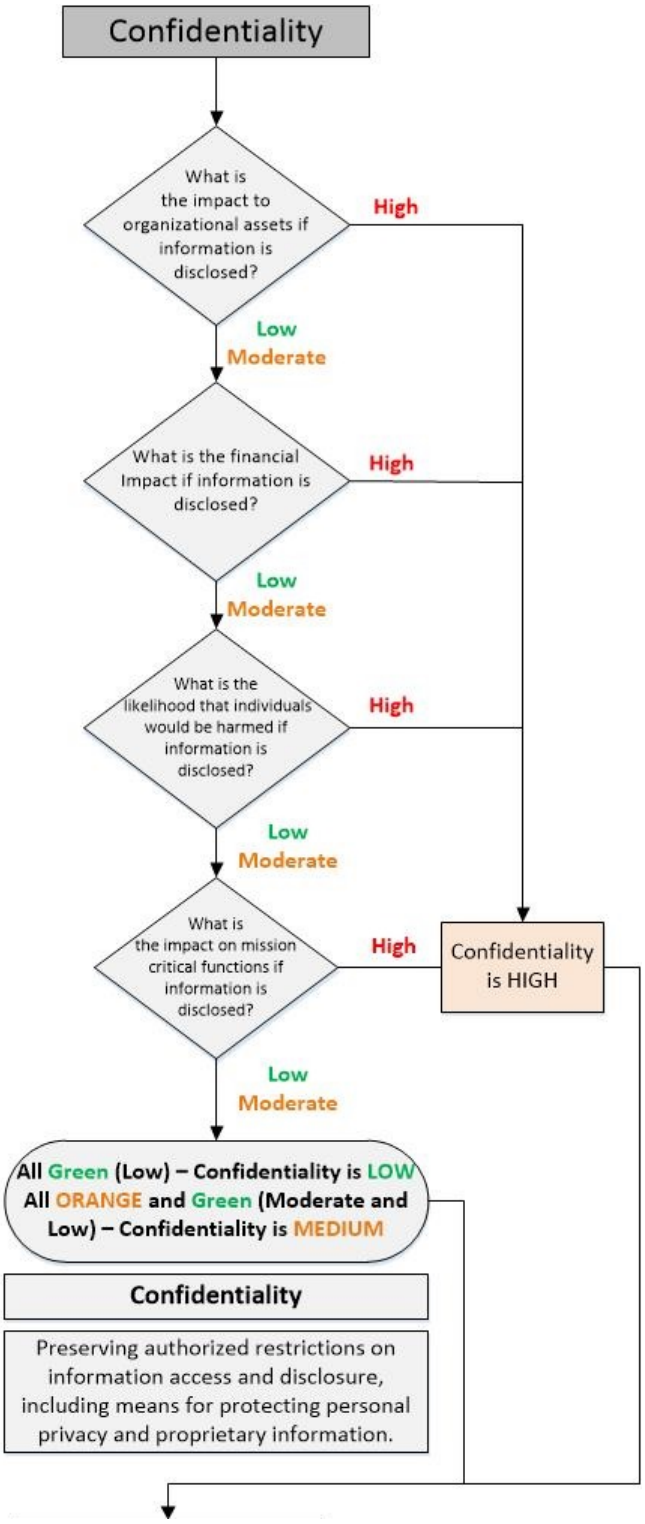
The information owner is responsible for determining the information's classification and how and by whom the information will be used.

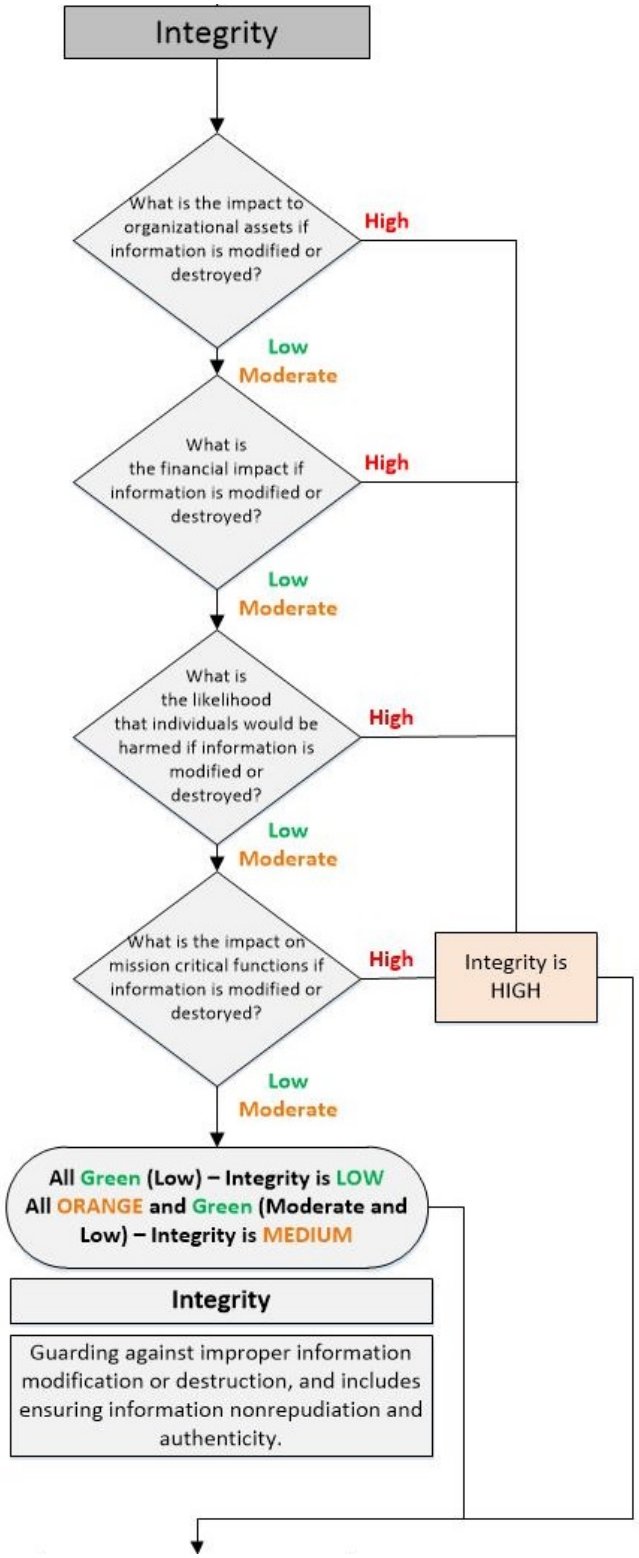
Example:

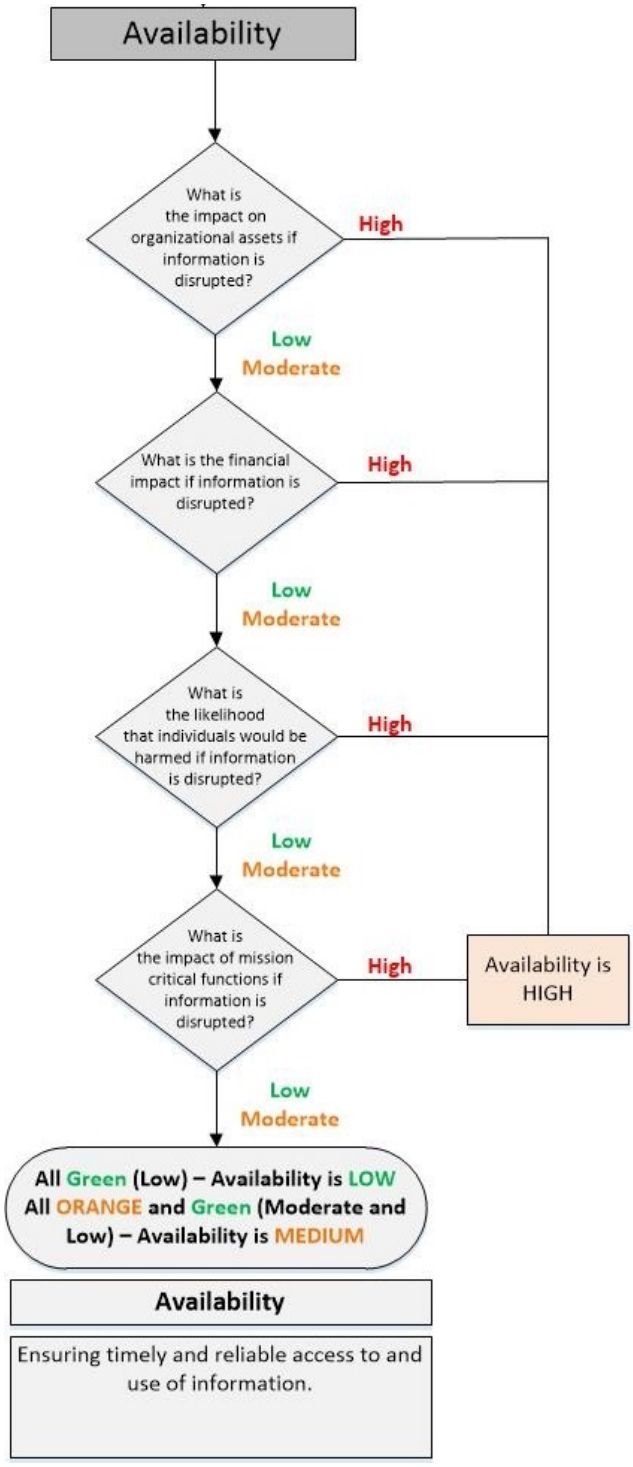
Asset Name	Asset Owner	Confidentiality	Ingetrity	Availability	Classification
Student Grades	Registrar				
Admission Data	VP of Admissions				
Annual Report	Board of Trustees				
Health Records	Health Director				

STEP 3 – EVALUATE DATA ASSET

Use the flowchart below to identify the levels of classification for the confidentiality, integrity and availability of each information asset. Classification of data will be based on specific, finite criteria as identified in the *Federal Information Processing Standard Publication 199 (FIPS-199).* Please see Appendix A for details on FIPS-199 categories.


Confidentiality
What is the impact to organizational assets if information is disclosed?
High
Low
Moderate
What is the financial Impact if information is disclosed?
High
Low
Moderate
What is the likelihood that individuals would be harmed if information is disclosed?
High
Low
Moderate
What is the impact on mission critical functions if information is disclosed?
High
Confidentiality is HIGH
Low
Moderate
All Green (Low) – Confidentiality is LOW
All ORANGE and Green (Moderate and Low) – Confidentiality is MEDIUM
Confidentiality
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.


Integrity
What is the impact to organizational assets if information is modified or destroyed?
High
Low
Moderate
What is the financial impact if information is modified or destroyed?
High
Low
Moderate
What is the likelihood that individuals would be harmed if information is modified or destroyed?
High
Low
Moderate
What is the impact on mission critical functions if information is modified or destoryed?
High
Integrity is HIGH
Low
Moderate
All Green (Low) – Integrity is LOW
All ORANGE and Green (Moderate and Low) – Integrity is MEDIUM
Integrity
Guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity.


Availability
What is the impact on organizational assets if information is disrupted?
High
Low
Moderate
What is the financial impact if information is disrupted?
High
Low
Moderate
What is the likelihood that individuals would be harmed if information is disrupted?
High
Low
Moderate
What is the impact of mission critical functions if information is disrupted?
High
Availability is HIGH
Low
Moderate
All Green (Low) – Availability is LOW
All ORANGE and Green (Moderate and Low) – Availability is MEDIUM
Availability
Ensuring timely and reliable access to and use of information.

Examples:

Asset Name	Asset Owner	Confidentiality	Ingetrity	Availability	Classification
Student Grades	Registrar	High	High	High	
Admission Data	VP of Admissions	Moderate	Moderate	Moderate	
Annual Report	Board of Trustees	Low	Low	Low	
Health Records	Health Director	High	Moderate	Moderate	

STEP 4 – ASSIGN DATA CLASSIFICATION

Classification of data asset will be based on the highest category assigned to Confidentiality, Integrity or Availability. If any category is rated High, the data asset shall be classified as Confidential. If all categories are rated Low, the data asset shall be classified as Public. All other data assets shall be classified as Sensitive.

Examples:

Asset Name	Asset Owner	Confidentiality	Ingetrity	Availability	Classification
Student Grades	Registrar	High	High	High	Confidential
Admission Data	VP of Admissions	Moderate	Moderate	Moderate	Sensitive
Annual Report	Board of Trustees	Low	Low	Low	Public
Health Records	Health Director	High	Moderate	Moderate	Confidential

STEP 5 – IMPLEMENT DATA HANDLING CONTROLS

Information assets shall be labelled (if possible) and handled according to their prescribed classification, including access controls, labeling, retention policies and destruction methods, among others. The following controls shall be applied to data assets, based on their classification:

	Confidential	Sensitive	Public
Non-Disclosure Agreement (NDA)	• NDA is required prior to access by non-Union employees	• NDA is required prior to access by non-Union employees	• N/A

	Confidential	Sensitive	Public
Access	• Strong password(s) • Access request, review, approval and termination process • Asset Owner-approved access • Non-Disclosure Agreement (NDA) for third-parties • Immediate retrieval when printing or faxing • Secure storage when not in use • Situational awareness for verbal communications	• Password(s) • Access request, review, approval and termination process • Secure storage when not in use • Situational awareness for verbal communications	• Access request, review, approval and termination process
Cloud-based Storage (DropBox, OneDrive, Google Drive)	• Only use Union's Google Drive	• Only use Union's Google Drive	• None
Email (with and without attachments)	• To other @union.edu addresses: Union's Google Mail solution • To non-@union.edu addresses: All information encrypted using MS Office password protection	• To other Union Employees: Union's Google Mail solution • To non-Union Employees: All information encrypted using MS Office password protection	• None
Encryption	• Encryption during creation, storage, processing and transmission • Encryption for third parties	• Encryption during transmission • Encryption for third parties	• None
Internal & External Network Transmission (wired & wireless)	• Encryption is required • Instant Messaging is prohibited • Non-IT approved FTP solutions are prohibited • Remote access should be used only when necessary and only with approved VPN and two-factor authentication solutions	• Encryption is required • Instant Messaging is prohibited • Non-IT approved FTP solutions are prohibited	• None
Faxing / Printing	• Verify destination printer • Attend fax/printer while printing	• Verify destination printer • Attend fax/printer while printing	• None

	Confidential	Sensitive	Public
Labelling	• Document watermark	• None	• None
Mobile Devices (iPhone, iPad, MP3 player, USB drive, etc.)	• Encryption is required	• Encryption is required	• None
Monitoring	• Security monitoring and alerting • Privileged identity monitoring	• None	• None
Removable Media (flash drives, jump drives, external hard drives, CD's, DVD's, etc.)	• Only use IT approved solutions	• Only use IT approved solutions	• None
Retention	• Backup testing and verification • Inclusion in Business Continuity and Disaster Recovery Plans • Redundancy or automatic failover • Offsite backup • Secure physical storage	• Backup testing and verification • Inclusion in Business Continuity and Disaster Recovery Plans	• None
Destruction	• Approved secure destruction solutions, including shredding and secure wiping	• Approved secure destruction solutions, including shredding and secure wiping	• None
Audit	• Annual controls audit	• Biennial controls audit	• None
Physical	• Secure courier when shipping • Media possession at all times • Mark "Open by Addressee Only" • Use "Certified Mail" and sealed, tamper- resistant envelopes for external mailings • Delivery confirmation is required	• Secure courier when shipping • Media possession at all times • Mark "Open by Addressee Only" • Use "Certified Mail" and sealed, tamper- resistant envelopes for external mailings • Delivery confirmation is required	• None

7.0 DATA CLASSIFICATION EXAMPLES

The following table depicts examples of sensitive data elements and their assigned classification:

DATA CLASS	SENSITIVE DATA ELEMENTS	Public	Sensitive	Confidential
Personally Identifiable Information	Social Security Number (SSN)			X
	Employer Identification Number (EIN)			X
	Driver's License (DL) Number			X
	Financial Account Number			X
	Payment Card Number (credit or debit)			X
	Government-Issued Identification (e.g., passport, permanent resident card, etc)			X
	Electronic Protected Health Information			X
	Birth Date			X
	First & Last Name			X
	Age			X
	Phone and/or Fax Number			X
	Home Address			X
	Gender			X
	Ethnicity			X
	Email Address			X
Other Employee-Data	Protected Data Related to Research		X	
	Compensation & Benefits Data			X
	Medical Data			X
	Workers Compensation Claim Data			X
	Education Data		X	
	Dependent or Beneficiary Data		X	
Student-Related Data	Academic Transcript			X
	Class Schedule			X
	Individual Grades			X
	Major	X		
	Degree	X		
	Advising Notes			X

DATA CLASS	SENSITIVE DATA ELEMENTS	Public	Sensitive	Confidential
Marketing Data	Business Plan (including marketing strategy)		X	
	Financial Data Related to Revenue Generation		X	
	Marketing Promotions Development		X	
	Internet-Facing Websites (e.g., institution website, social networks, blogs, promotions, etc.)	X		
	News Releases	X		
Networking & Infrastructure Data	Username & Password Pairs			X
	Public Key Infrastructure (PKI) Cryptographic Keys (public and private)			X
	Hardware or Software Tokens (multifactor authentication)			X
	System Configuration Settings		X	
	Regulatory Compliance Data		X	
	Internal IP Addresses		X	
	Privileged Account Usernames		X	
	Service Provider Account Numbers		X	
IP	Formulas			X
	Research and Development			X
Strategic Financial Data	Corporate Tax Return Information			X
	Legal Billings			X
	Budget-Related Data			X
	Unannounced Merger and Acquisition Information			X
	Trade Secrets (e.g., design diagrams, competitive information, etc.)			X
Operating Financial Data	Electronic Payment Information (Wire Payment / ACH)			X
	Paychecks			X
	Incentives or Bonuses (amounts or percentages)			X
	Stock Dividend Information			X
	Bank Account Information			X
	Investment-Related Activity			X
	Account Information (e.g., stocks, bonds, mutual funds, money markets, etc.)			X
	Debt Amount Information			X
	SEC Disclosure Information			X

8.0 REFERENCES

- Policy – 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)

9.0 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	04-19-16	GreyCastle Security	Union College Updates
1.11	05-09-16	GreyCastle Security	Union College Updates
1.12		GreyCastle Security	Updates based on DC Workshop
1.13	09-14-17	GreyCastle Security	Review and update of Union Changes
1.14	09-18-17	GreyCastle Security	Union College Updates

APPENDIX A – FIPS 199 CATEGORIES

	INFORMATION CLASSIFICATION CATEGORIES		
	LOW	**MODERATE**	**HIGH**
CONFIDENTIALITY Consider impact of unauthorized disclosure on factors such as: • Health and Safety • Financial Loss • SE Mission/Programs • Public Trust	The unauthorized access or disclosure of information would have ***minimal or no impact*** to the organization, its critical functions, workforce, business partners and/or its customers.	The unauthorized access or disclosure of information would have only ***limited impact*** to the organization, its critical functions, workforce, business partners and/or its customers.	The unauthorized access or disclosure of PPSI or other information would have a ***severe impact*** on the organization, its critical functions, workforce, business partners and/or its customers.
INTEGRITY Consider impact of unauthorized modification or destruction on factors such as: • Health and Safety • Financial Loss • SE Mission/Programs • Public Trust	The unauthorized modification or destruction of information would have ***minimal or no impact*** to the organization, its critical functions, workforce, business partners and/or its customers.	The unauthorized modification or destruction of information would have only ***limited impact*** to the organization, its critical functions, workforce, business partners and/or its customers.	The unauthorized modification or destruction of information would have a ***severe impact*** on the organization, its critical functions, workforce, business partners and/or its customers.
AVAILABILITY Consider impact of untimely or unreliable access to information on factors such as: • Health and Safety • Financial Loss • SE Mission/Programs ▪ Public Trust	The disruption of access to or use of information would have ***minimal or no impact*** to the organization, its critical functions, workforce, business partners and/or its customers.	The disruption of access to or use of information would have only ***limited impact*** to the organization, its critical functions, workforce, business partners and/or its customers.	The disruption of access to or use of information would have a ***severe impact*** on the organization, its critical functions, workforce, business partners and/or its customers.