CITY UNIVERSITY OF NEW YORK INFORMATION SECURITY POLICY	
Data Classification Standard	**Issue Date:** 8/19/2019
	Issued By: University Chief Information Officer **Policy Owner:** Computing and Information Services

Purpose and Background:

This standard defines a framework for categorizing the University's institutional data assets by establishing a data classification standard. It is the intention of this standard to promote the widest possible use of *University Data* in support of University academic, research and administrative objectives by providing the uniform basis to define appropriate levels of protection and to comply with applicable laws and regulations.

This standard is derived from a variety of sources, including FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, NYS-S14-002, the *New York State Information Classification Technology Standard*, NIST SP800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* as well as the data classification standards of other institutions of higher education.

Scope:

This standard applies to all *University Entities* and governs all University Data, electronic or non-electronic, which is processed, created, collected, stored or archived by the University. Any individual who uses, stores or transmits University Data shares the responsibility to appropriately safeguard such data.

Statement:

This Data Classification Standard categorizes types of data for determining security measures that correspond to its sensitivity and the level of risk should the data be inappropriately exposed, altered, purged or unavailable. The *Data Owner* is the primary party responsible to use this standard to evaluate and classify University Data within its purview according to the classification categories outlined below. It is appropriate for the Data Owner to confer with *Subject Matter Experts* who possess in-depth knowledge regarding its information assets.

A *dataset* or system must be classified to reflect the highest classification required of any data element that can be present. For example, if a dataset contains a student's name and optional

social security number, the dataset should be classified as Confidential Data even though a student's name may, by itself, be classified at a less restrictive classification level. Equally important, data must be classified according to the lowest (least restrictive) category appropriate to that data in its context.

Three data classification categories are defined below.

- **Confidential Data:** Data shall be classified as ***Confidential*** when the unauthorized disclosure, alteration or destruction of that data could result in a **significant level of risk** to the University. Significant risk includes but is not limited to: substantial financial, reputational and/or personal privacy loss; impairing the functions of the University; or presenting a legal or financial liability. Confidential Data requires the highest level of protection and control. See Appendix A for a list of predefined types of Confidential Data.

- **Sensitive Data:** Data shall be classified as ***Sensitive*** when the unauthorized disclosure, alteration or destruction of that data could result in a **moderate to low level of risk** to the University. All data that is not classified as Confidential Data or Public Data should be considered Sensitive Data. Sensitive Data requires moderate protection. See Appendix B for examples of Sensitive Data.

- **Public Data:** Data shall be classified as ***Public*** when the unauthorized disclosure, alteration or destruction of that data could result in **little or no risk** to the University. Examples of Public Data include data published on public websites, press releases, course catalog information, job postings, etc. While access control measures may or may not be required for particular Public Data, protections to ensure the integrity and/or availability of certain Public Data may be appropriate.

Non-Public University Information

The definition of Non-Public University Information (NPUI), as defined in the *CUNY IT Security Procedures – General (June 25, 2014)*, is superseded by this standard. The combined Confidential and Sensitive data classifications are substantially comparable to the less-detailed NPUI definition and may be used to guide compliance with the Procedures until they are revised.

Reclassification

On an ongoing basis, Data Owners should evaluate the classification of their University Data to ensure the assigned classification remains appropriate based on any changes to legal and contractual obligations as well as changes in the use of the dataset and its value to the University.

If a Data Owner determines that the classification of a certain data set has changed, an analysis of security protections should be performed to determine if modifications are necessary to align

with the new classification. Any required changes to the protection profile should be implemented in a timely manner.

Related Information

CUNY IT Policies - http://www.cuny.edu/about/administration/offices/CIS/policies.html

CUNY IT Security Policies and Procedures – https://security.cuny.edu

CUNY Records Retention Schedule – http://policy.cuny.edu/schedule/

FERPA - http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Payment Card Industry Data Security Standard - https://www.pcisecuritystandards.org/pci_security/

FIPS 199 - Security Categorization of Federal Information and Information Systems https://csrc.nist.gov/publications/detail/fips/199/final

SP 800-122 - Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) https://csrc.nist.gov/publications/detail/sp/800-122/final

NY State Information Technology Standard – Information Classification https://its.ny.gov/document/information-classification-standard

Definitions and Terms

Affiliate or Affiliated Organization: Any organization associated with the University that uses University resources to create, access, store or manage University Data to carry out its business functions. This applies to all third party vendors under a contractual agreement.

Data Element: A unit of data that refers to one separate item of information, such as name, address, date of birth, etc.

Data Owner: The University Entity (typically a function or department) that can authorize or deny access to certain data, can delegate custody of that data and is accountable for its accuracy, integrity and timeliness. The Data Owner is responsible to classify its data so that appropriate safeguards are applied to protect its data resources. Common examples of Data Owners:

Data Classification Standard

Description	Common Data Owner(s)
Student Records	Registrar, Enrollment Management, Bursar, Student Finance, Student Affairs
Employee Records	Human Resources
Research Data	Researcher, Principal Investigator
Financial Data	Finance, Business Office, Procurement
Academic	Faculty, Department Chair, Dean, Provost, Academic Affairs

Data User: Creates, accesses and alters data as well as uses data resources and is responsible to comply with data use requirements.

Dataset: A collection of *Data Elements*, such as data contained in a file, document or database or as aggregated in any form.

Personally Identifiable Information (PII): Any information that permits the identity of an individual to be directly or indirectly inferred.

Subject Matter Expert: A subject matter expert (SME) is an individual with an in-depth, authoritative understanding of a particular functional area such as registration, enrollment, finance, etc.

University Data: Any CUNY institutional data related to CUNY's academic, research and administrative functions either stored on CUNY information technology systems or maintained by, or on behalf of, CUNY faculty, staff, students and affiliates in any format or location.

University Entities: All colleges, academic and administrative departments and affiliates.

Data Classification Standard

Appendix – A

Predefined Types of Confidential Data

1. **Personally Identifiable Information (PII)**

   PII is any information about an individual that can be used to distinguish or trace a natural individual's identity.

   The following list contains examples of information that may be considered PII.

   - Name, such as full name, preferred name, maiden name, mother's maiden name, or alias
   - Personal identification number, such as social security number (SSN), passport number, state-issued driver's license number, state-issued non-driver identification card number, taxpayer identification number, patient identification number, and financial account or credit card number
   - Address information, such as home street address or personal email address
   - Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address and other persistent static identifier that consistently links to a particular person or a small, well-defined group of people
   - Telephone numbers, including mobile, business, and personal numbers
   - Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry)
   - Information identifying personally owned property, such as vehicle registration number or title number and related information
   - Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

   Contextual Considerations

   The context, nature and combinations of PII data elements present are factors relevant to the level of confidentiality for a particular use. For example, a list of names contained within a file can be classified differently depending upon the nature of the list:

Example Context	Classification
Individuals with a criminal record	Confidential
Students requiring behavioral intervention	Confidential

Example Context	Classification
Immigration status	Confidential
Employees with poor performance ratings	Confidential
Compliance training participants	Sensitive
Attendees at a public meeting	Public

It is therefore relevant for Data Owners to consider context when determining an appropriate data classification for particular instances of PII. PII containing personal identification numbers shall be classified Confidential Data regardless of context.

2. New York State Private Information

New York State data breach notification law defines "private information" as any information that permits the identity of an individual to be inferred (e.g., name) in combination with one or more of the following data elements:

- Social Security Number
- State-issued driver's license number
- State-issued non-driver identification card number
- Financial account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account

Data containing New York State private information is classified Confidential Data regardless of context.

3. Personally Identifiable Education Records

Student educational records that require protection under the Federal Educational Rights and Privacy Act (FERPA). Examples include class rosters, test scores, grades and financial aid information that can be associated with an individual.

FERPA permits certain PII defined as "directory information" to be disclosed to outside organizations and/or inquirers without prior student consent, unless a student requests such information be withheld. Directory information is information that is generally not considered harmful or an invasion of privacy if released. Such directory information should be classified as Sensitive.

Student ID

A student's unique ID number and user ID (e.g., CUNYfirst EMPLID, account username, etc.) can be considered directory information as above so long as it cannot be used to gain

access to education records except when used in conjunction with one or more factors that authenticate the user's identity, such as a password, personal identification number (PIN), or other factor known or possessed only by the authorized user.

4. **Protected Health Information (PHI)**

   Health information about an individual including medical records, health status, and records covered by health privacy laws.

5. **Citizenship**

   Information about an individual's US citizenship status, immigration information, etc.

6. **Personnel Records**

   Personnel records of a confidential nature including disciplinary and behavioral matters, evaluations, background checks, criminal records, police, court and investigation records, etc.

7. **Payment Card Information**

   Payment cardholder information requiring protection under the Payment Card Industry Data Security Standard (PCI DSS), such as credit and debit card numbers, card expiration dates, etc.

   This includes the credit/debit card number (also referred to as a primary account number or PAN) in combination with one or more of the following data elements:

   - Cardholder name
   - Service code
   - Expiration date
   - CVC2, CVV2 or CID value
   - PIN or PIN block
   - Contents of a card's magnetic stripe

8. **Covered Financial Information**

   Regulated financial information, such as student financial aid records requiring protection under the Gramm-Leach-Bliley Act (GLBA), and other relevant regulations.

9. **Restricted Procurement Information**

   Procurement information that must remain confidential as defined by New York State finance law, including RFP bid responses during the "restricted period."

10. Federal Tax Information ("FTI")

FTI is defined as any return, return information or taxpayer return information that is entrusted to the University by a taxpayer or the Internal Revenue Services. See Internal Revenue Service Publication 1075 Exhibit 2 for more information.

11. Intellectual Property

Trade secrets, technology, designs, models and other information that may be relevant for the creation of a University, faculty or student owned patent.

12. Personally Identifiable and Restricted Research Data

Human subject and other research data containing PII (i.e., not de-identified) and/or licensed under a restricted data use agreement or other applicable restriction mandated by the CUNY Human Research Protection Program (HRPP) / Institutional Review Board (IRB).

13. Passwords and Access Codes

Any information held in confidence by an individual used to verify the identity of the person, such as passwords and access codes. Such verifiers can also be used to prove the identity of a system or service. Examples include:

- Passwords
- PINs
- Access codes
- Tokens
- Shared secrets
- Cryptographic private keys

14. Export Controlled Materials

Export Controlled Materials is defined as any information or materials that are subject to United States export control regulations including, but not limited to, the Export Administration Regulations ("EAR") published by the U.S. Department of Commerce and the International Traffic in Arms Regulations ("ITAR") published by the U.S. Department of State. See the Information and Guidelines on Federal Export Control Laws and Regulations, published by the Office of Sponsored Programs, for more information.

15. Other Confidential Information

Any data that by its nature requires confidentiality or that the University is required to maintain confidentially, such as data subject to a confidentiality agreement executed by the University.

Data Classification Standard

Appendix – B

Examples of Sensitive Data

- Email and other communications regarding internal matters which have not been specifically approved for public release
- Proprietary financial, budgetary or personnel information not explicitly approved by authorized parties for public release
- Identities of donors or other third-party partner information maintained by the University not specifically designated for public release
- Information designated as "Directory Information" under FERPA. Directory information that is withheld by the request of a student should be classified as Confidential Data. (See "Appendix A Personally Identifiable Education Records")
- Examinations (questions and answers)
- IT system configurations and logs not containing Confidential Data
- Business recovery and emergency response plans
- Any other non-Confidential Data that should not be distributed publicly

Data Classification Standard

Appendix – C

Examples of Public Data

- The content of public websites, like www.cuny.edu
- Course curriculums
- Class schedules (not student specific)
- Course catalogs
- Information about campus activities, clubs and organizations
- University policies
- Academic calendars
- Academic programs
- Information on how to access educational resources
- Publicly accessible services
- Press releases
- Public communications and advisories
- Information that by law or regulation is required to be publicly disclosed
- Scholarly publications, research data and findings not otherwise classified as Confidential or Sensitive Data.

Note: Though, by definition, disclosure of Public Data must present little or no risk to the University (irrespective of whether such disclosure is intended or desired), it is nevertheless appropriate for Data Users and Data Owners to apply access restrictions for certain Public Data. Examples include draft or provisional documents; scholarly publications during development, collaboration and peer review; targeted communications and other Public Data documents prior to approval for general release or publication.