Data Classification Policy

Policy Statement
Data classification is a method of assigning a level of sensitivity to data. The classification of the data determines the extent to which it needs to be controlled and secured. This policy defines the required data protection criteria based on its classification and sensitivity.

Reason for the Policy
The classification of data, information, and documents is essential to differentiate between non-sensitive and sensitive / confidential information. When data is stored, created, amended or transmitted, it should be appropriately classified and protected in accordance to the sensitivity level.

Primary Guidance to Which This Policy Responds
This policy responds to all applicable federal and state statutes pertaining to protection of sensitive and confidential information. These statutes include, but are not limited to, the New York State Law, the New York State Information Security Breach and Notification Act, the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Gramm-Leach-Bliley Act (GLBA), and Payment Card Industry Data Security Standard (PCI DSS).

Responsible University Office & Officer
The office of Columbia University Information Technology Security is responsible for the maintenance of this policy, and for responding to questions regarding this policy. The Chief Information Security Officer (CISO) is the responsible officer.

Revision History
This policy was established in December 2007.

Who is Governed by This Policy
This policy applies to all individuals who access, use, or control Columbia University electronic information resources. Those individuals covered include, but are not limited to faculty, staff, students, those working on behalf of the University, and individuals authorized by affiliated institutions and organizations.

Who Should Know This Policy
Anyone who accesses, uses, or controls Columbia University electronic information resources should be familiar with this policy.

Exclusions & Special Situations
Existing systems and applications containing sensitive and confidential information which cannot use encryption because of technology limitation but have compensating controls may be granted special waiver. However, these systems and applications must still be thoroughly risk assessed to ensure that major risks are addressed via compensating controls to protect the data in lieu of not using encryption.
Policy Text

Data must be maintained in a secured, accurate, and reliable manner and be readily available for authorized use. Data security measures need to be implemented commensurate with data value, sensitivity, and risk. Departments should carefully evaluate the appropriate data classification category for their information. The classification level for individual information can be derived by systematically considering the impact to Columbia University should the information fall victim to security risks (e.g., unauthorized disclosure, unauthorized data manipulation, loss of data, etc.).

This document covers all information regardless of storage medium (e.g., paper, fiche, electronic tape, cartridge, disk, and CD / DVD) and regardless of form (e.g., text, graphic, video, and voice).

In order to protect information from unauthorized disclosure, use, modification or deletion, use the designated information classification system.

- Category HS – Highest Sensitivity (Confidential / Sensitive Data)
- Category MS – Moderate Sensitivity (Internal / Official Use Only Data)
- Category NS – Non-Sensitive (Public Data)

Use criteria in Appendices A – “Data Classification Categories” and B – “Data Classification Table” at the end of this document to determine which data category is appropriate and the protection levels required.

Category HS data must not be collected or stored unless it is for business and/or legal requirements.

Aggregates of data should be classified based upon the most secure classification level; in other words, when data of mixed classification exist in the same document (e.g., file, report, etc.), the document should have the highest level of classification.

In the event a particular data has not been classified, as an interim control, it should be considered as either highly sensitive or moderately sensitive until it is properly classified.

The offices of the General Counsel, Columbia University Information Technology Security, and Public Safety must be notified immediately if Category HS data is lost, disclosed to unauthorized parties or suspected of being lost or disclosed to unauthorized parties, or if any unauthorized use of Columbia University's information systems has taken place or is suspected of taking place. See the “Electronic Data Security Breach Reporting and Response Policy” for reporting process.

Responsibilities

All members of Columbia University’s community have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored or used by the University, irrespective of the medium on which the data resides and regardless of format (e.g., in electronic, paper or other physical form).
Departments are responsible for implementing appropriate managerial, operational, physical, and technical controls for access to, use of, transmission of, and disposal of Columbia University data in compliance with this policy.

The following roles and responsibilities are established for carrying out this policy:

**Data Trustees / Owners:**
Data Trustees / Owners are senior University officials (e.g., Provosts, Deans, VPs, AVPs, or their designees) within each businesses and/or operational units in Columbia University. Data Trustee / Owner responsibilities include: assigning data stewards, establishing departmental data protection policies and procedures, and promoting data resource management for the good of the entire University.

**Data Stewards:**
Data Stewards are University officials (e.g., Directors, Managers, or their designees) having direct operational level responsibility for information management. Data stewards are responsible for: working with Data Trustee / Owner to classify data, approving data access on behalf of Data Trustee / Owner, determining / specifying user access level(s), implementing and enforcing departmental policy and procedures.

**Data Administrators:**
Data Administrators are responsible for providing a secure infrastructure in support of the data including, but not limited to, providing physical security, backup and recovery processes, granting access privileges as authorized by data owners or their designees (usually data stewards), and implementing and administering controls over the information.

**Data Users:**
Data users are individuals who need and use Columbia University data as part of their assigned duties or in fulfillment of assigned roles or functions within the University community. Individuals who are given access to sensitive data have a position of special trust, and as such, are responsible for protecting the security and integrity of those data.

Anyone who has intentionally breached the confidentiality and/or compromised the integrity of protected data / information (e.g., category HS data) may be subject to disciplinary action and/or sanctions up to, and including discharge or dismissal in accordance to Columbia University policy and procedures. Additionally, breach of confidentiality and/or compromising integrity of data / information that are protected by law, acts, or regulations, will result in criminal prosecution.

**Definitions**
*Data* is defined as any information within Columbia University's purview, including student record data, personnel data, financial data (budget and payroll), student life data, departmental administrative data, legal files, research data, proprietary data, and all other data that pertains to, or supports the administration of the University.
Electronic Information Resources include data, networks, computers, and other devices that store or display data, communications and transmission devices, and software used on such devices.

Contacts
For questions or comments:
Columbia University Information Technology
   Web:  http://www.columbia.edu/cuit/support/
   Email: security@columbia.edu
   Telephone: 212-854-1919

Cross References to Related Policies
For CUIT Security Policies, see the University Administrative Policy Library, CU Information Technology section:

http://www.columbia.edu/cu/administration/policylibrary/responsible_office/cuit.html

The “Encryption Policy”

Applicable Acts, Regulations, and Laws:

- NY State Law: Chapter 16, Article 1, Title 1, Section 2b
  http://caselaw.lp.findlaw.com/nycodes/c30/a3.html
- Gramm-Leach-Bliley Act (GLBA)
  http://www.ftc.gov/privacy/privacyinitiatives/glbact.html
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
  http://www.cms.hhs.gov/HIPAAGenInfo/02_TheHIPAALawandRelated%20Information.asp#TopOfPage
- Payment Card Industry Data Security Standard (PCI DSS)
  https://www.pcisecuritystandards.org/tech/