Data Sanitization / Disposal of Electronic Equipment Policy

Effective Date: January 1, 2008

Policy Statement
Data sanitization is the deliberate and permanent removal or destruction of the data on a storage media device. When a storage media device becomes obsolete or the sensitive data is no longer needed, all sensitive data must be effectively removed from the storage media before the devices are reused or discarded. This policy defines the appropriate data sanitization and disposal methods based on the data classification and sensitivity level at Columbia University.

Reason for the Policy
This policy ensures that sensitive data is not inappropriately released. Sensitive data may include: information classified by the University's administration; information protected by laws such as the Family Educational Rights and Privacy Act (FERPA); the Health Insurance Portability and Accountability Act of 1996 (HIPAA); the Gramm-Leach-Bliley Act (GLBA); information that could lead to identity theft; information that could contribute to problematic or sensitive situations for the University; and/or information leading to the loss of personal privacy, licensed software, or restricted intellectual property. The sensitive data could be stored in devices, including but not exclusive to: desktop and laptop computer hard drives, removable storage devices (e.g., a CD, DVD, floppy disk, Zip drive, external hard drive, USB disk or flash drive), or any devices with storage capabilities (e.g., mobile devices, copier, etc.).

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, New York State Law, the New York State Information Security Breach and Notification Act, FERPA, HIPAA, GLBA, and the Payment Card Industry Data Security Standard (PCI DSS).

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

Revision History
This policy was established in January 2008. The policy was revised in August 2010 to expand the inclusion of any devices with storage capabilities, update to the special situations section to include handling of devices with encryption software, and added Appendix A - copier hard drives disposal process and procedures.

Who is Governed by This Policy
This policy applies to all individuals who access, use or control Columbia University’s electronic information resources. Those individuals covered include, but are not limited to, faculty, staff, students, contractors, consultants, those working on behalf of the University and/or individuals authorized by affiliated institutions and organizations.
Who Should Know This Policy
Anyone who accesses, uses or controls Columbia University’s electronic information resources should be familiar with this policy.

Exclusions and Special Situations
Any storage device that has been fully encrypted using Columbia University approved encryption software (e.g., GuardianEdge, DOSS, etc.) does not need to be erased, provided that the encryption password is not included with, nor can be recovered from the device to be disposed.

For disposal of copiers not outfitted with DOSS, compliance with the process and procedure in appendix A - copier hard drives disposal process and procedures is mandatory.

Policy Text
This policy covers all information regardless of storage medium (e.g., paper, fiche, electronic tape, cartridge, disk, CD, DVD, external drive) and regardless of form (e.g., text, graphic, video, voice). When sensitive documents and data are no longer required, they must be sanitized in accordance to the sanitization method below.

The data sanitization process involves the following steps:
- Assessing the sensitivity and security category of the stored data;
- Selecting the appropriate data sanitization method based on the category;
- Sanitizing the media; and
- Verifying the result.

See the “Data Classification Policy” for details of the three data classification categories:

- Category HS – Highest Sensitivity (Confidential / Sensitive Data)
- Category MS – Moderate Sensitivity (Internal / Official Use Only Data)
- Category NS – Not Sensitive (Public Data)

Based on this data classification, electronic data on magnetic storage and media devices should be sanitized using the following methods:

Categories HS and MS sanitization method
Use specialized data removal software to remove the data more robustly than simply deleting and/or reformattting the media device before the media device is reused. Data removal software (Darik’s Boot and Nuke, or DBAN), which is both PC and Macintosh compatible, is available online from CUIT (http://www.columbia.edu/acis/security/download/).

Note: If a computer was used to access sensitive information, there is a high likelihood that the system retained that information on the hard drive even after the user has exited the program. Therefore, always use the Categories HS and MS sanitization method to cleanse the equipment prior to reuse and/or disposal.

Category NS sanitization method
The media should be reformatted before it is reused.

**Multiple categories**
When a storage media device contains data of multiple categories, use the sanitization method for categories HS and MS.

**Disposal process**
When discarding any equipment with a storage media device, always verify whether the device contains any data classified as Category HS or MS and then apply the appropriate data sanitization method. Remove the storage media device from the equipment, if possible, and discard it separately and more securely (e.g., disintegration and/or pulverization) making the device unsalvageable and unusable.

For discarding non-reusable media (e.g., CD+/R, DVD+/R, paper, fiche, etc.) that contains sensitive data, take steps to adequately destroy the media (e.g., disintegration, pulverization or cross-cut shredding) to physically make the device unsalvageable and usable.

**Responsibilities**
All members of the University community have a responsibility to protect the confidentiality, integrity and availability of data stored or used by Columbia, irrespective of the media 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 disposal of University data in compliance with this policy.

Failure to abide by this policy may be subject to disciplinary action and/or sanctions up to and including discharge or dismissal in accordance to University policy and procedures. Additionally, intentional negligence that results in breach of confidentiality of data that are protected by law, acts or regulations can also 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/](http://www.columbia.edu/cuit/support/)
Email: security@columbia.edu
Telephone: 212-854-1919
Cross References to Related Policies
For guidelines and details relating to data classification, see the “Data Classification Policy.”

http://policylibrary.columbia.edu/data-classification-policy

Applicable Acts, Regulations and Laws:

- 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/security_standards/pci_dss.shtml