COLUMBIA UNIVERSITY
SANITIZATION AND DISPOSAL OF INFORMATION RESOURCES POLICY

Published: October 2013
Revised: November 2014

I. Introduction

A large volume of Data is stored on Systems (as each such term is defined in the Columbia University Information Security Charter (the “Charter”) http://policylibrary.columbia.edu/information-security-charter throughout Columbia University. A substantial amount of this Data consists of Sensitive Data or Confidential Data (as each such term is defined in the Charter). Unauthorized disclosure of such Data may expose the University to legal liability. Data sanitization is the deliberate and permanent removal of Data from an Information Resource. This Policy defines the appropriate sanitization and disposal methods to be used.

Capitalized terms used herein without definition are defined in the Charter.

II. Policy History

The effective date of this Policy is November 1, 2013. This Policy and the other Information Security Policies replace (A) the following University Policies:

- Data Sanitization and Disposal of Electronic Equipment Policy, dated January 1, 2008, as amended in February 2008
- Electronic Information Resources Security Policy, dated March 1, 2007

and (B) the following CUMC Policy:

- Information Security: Backup, Device and Media Controls

III. Policy Text

Each System Owner, Data Owner, IT Custodian and User is responsible for determining if Sensitive Data or Confidential Data is present on the Information Resource by, for example, periodically scanning the Information Resource using software provided by CUIT or CUMC IT, and sanitizing all Information Resources with hard drives and Removable Media under his/her control prior to removal from the University in accordance with the following guidelines:

A. Non-Sensitive and Non-Confidential Data.

Data other than Sensitive Data or Confidential Data may be deleted and/or reformatted.

B. Sensitive Data and Confidential Data.
Sensitive Data and Confidential Data must be sanitized or disposed of in a manner that leaves the Data fully unrecoverable. Except as provided below, this can be accomplished by using one of the following methods:

- Information Security Office-approved destruction hardware to physically render the Data storage media inoperable, such as degaussing, shredding, pulverizing or melting;
- Release of the Information Resource containing storage media to CUIT or CUMC IT for destruction and disposal; or

Sensitive Data constituting EPHI must be sanitized and disposed of in accordance with the CUMC Information Security Procedures [https://secure.cumc.columbia.edu/cumcit/secure/policy/procedures.html](https://secure.cumc.columbia.edu/cumcit/secure/policy/procedures.html).

All paper based Sensitive Data or Confidential Data must be destroyed using cross-shredding or through a contract with an Information Security Office approved-vendor.

IV. **Cross References to Related Policies and Other Documentation**

The Information Security Policies and certain additional documentation referred to in this Policy are listed in Appendix A hereto.
Appendix A

Related Policies and Other Documentation

CUIT Data Deletion Software
http://cuit.columbia.edu/cuit/it-security-practices/physical-security/secure-deletion-dban

CUMC Data Disposal Process
https://secure.cumc.columbia.edu/cumcit/secure/policy/disposal.html

CUMC Information Security Procedures
https://secure.cumc.columbia.edu/cumcit/secure/policy/procedures.html

Data Classification Policy
http://policylibrary.columbia.edu/data-classification-policy

Information Security Charter
http://policylibrary.columbia.edu/information-security-charter