COLLEGE OF SCIENCE DATA SANATIZATION POLICY

Policy Number: COS-1001

Policy Subject: Disposal and Reuse of COS Data Storage Devices

Responsible Office: Director of I.T. and Security, College of Science

Related Policies:
- University Policy 1312 Physical and Logical Access Security
- University Policy 1114 Data Stewardship
- University Policy 1124 University Owned Cellular Equipment

I. SCOPE

This Policy applies to all academic and operational departments and offices of the College of Science at George Mason University. The policies and procedures provided herein apply to all College of Science faculty, staff, students, visitors and contractors.

This policy governs the disposal or reuse of all COS managed data storage media.

II. POLICY STATEMENT

The College of Science handles a variety of data and software essential to the performance of College business. This policy is created in order to eliminate the potential security risks for the COS related to the violation of software licensing agreements and the unauthorized disclosure of information such as personally identifiable data, research information, copyrights, and other intellectual property that might be stored on electronic media.

III. DEFINITIONS

Data storage device: any electronic media including but not limited to: disk drives, flash memory devices, usb devices, memory cards, cell phones, and PDAs.

IT Coordinator: Staff or faculty member designated by a Chair or Director who serves as a contact point for ITU and is asked to coordinate informational and technology requirements for their unit.
**Equipment Liason:** Staff or faculty member designated by a Chair or Director

**Acceptable sanitization software:** Secure erasure software used by the COS which includes
- Darik’s Boot and Nuke (DBAN) [http://www.dban.org](http://www.dban.org)
- Roddkil’s Disk Wipe [http://www.roadkil.net](http://www.roadkil.net)
- SDelete [http://technet.microsoft.com](http://technet.microsoft.com)
- Other software may be approved by the COS on ad-hoc basis

**IV. RESPONSIBILITIES**

End Users: Per University Policy Number 1114 “All IT System Users, not just Data Owners, Data Custodians, or Data Processors, are responsible for the security and privacy of data they access or store…” . All COS end users must consult their Equipment Liason, IT Coordinator, or the COS Director Information Technology and Security office, to ensure proper procedure is followed before the surplus, reassignment or disposal of any data storage assets owned by the University.

IT Coordinators, Equipment Liasons, and Systems Administrators are responsible for ensuring data sanitization of all COS owned data storage media before surplus, reassignment or disposal. In addition each IT Coordinator, Equipment Liason, or Systems Administrator shall inform the Director of Information Technology and Security of changes made to asset inventories in accordance with this policy.

**V. COMPLIANCE**

Equipment Liasons must retain copies of all Equipment Surplus and Interdepartmental Equipment Transfer forms annotated to include type and number of included data storage media, software used to sanitize said data storage media, date of sanitization, printed name and signature of the party performing sanitization.

This policy does not apply to initial assignment of new assets via Equipment Surplus or Interdepartmental Equipment Transfer forms.

**VI. REVIEW and UPDATE**

This Policy will be reviewed annually in July.

**VII. EFFECTIVE DATE**

The policies herein are effective February 24, 2014

Approved:
Justin Brown
Director I.T. and Security, College of Science
Date approved: February 24 2014