

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	October 2004
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.22	Storage Media Control	Responsibility:	Chief Information Security Officer

STORAGE MEDIA CONTROL

Overview

This policy pertains to the transport, repurposing and/or disposal of data storage devices. While the primary concern is “confidential” and “confidential/high risk” information, the policy applies to all storage media regardless of data classification, see the *Handbook of Operating Procedures* (HOP), [Section 5.8.21](#), “Data Classification” for more details.

Policy

Prior to disposal or repurposing storage media, original records subject to retention requirements must be copied to an alternative storage device, see the HOP, [Section 2.2.1](#), “Records and Information Management and Retention”. The policy mandates that original records must be accessible and retrievable for mandated retention periods, as documented in the institution’s [“Records Retention Schedule”](#). The alternative data device and all other removable media must be protected commensurate with the data stored on them.

- **DISPOSAL:** Prior to disposal of data storage media through the institution’s surplus property operation, the department must certify that no data (Health Science Center information or applications) remains on the media or device. For common rotating magnetic media (hard drives), the departmental Technical Support Representative (TSR) is authorized to use software designated by the Information Security Office that will destroy all data on the drive. Information System owners must remove all data contained on storage media within the information system prior to transferring it to the Health Science Center Warehouse. Additionally, the Information System owner must tag the system with their department ID, their full name (printed), initials, badge number and date that the data on the storage media was removed. See [Media Control \(Accountability\) Security Standard](#) for more details.
- **REPURPOSING:** Prior to repurposing a storage device or media (e.g., a new application on an existing computer) that previously contained “confidential” or “confidential/high risk”

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	October 2004
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.22	Storage Media Control	Responsibility:	Chief Information Security Officer

information, the information on the media must be completely destroyed using a process acceptable to the Information Security Office.

DATA/MEDIA TRANSPORT RESPONSIBILITIES: When using storage devices and removable media to transport and store “confidential/high risk” data, mechanisms must be in place to hold users accountable to the data owner for the data and media. This includes, but is not limited to, movement of the media, its storage, its transfer to other parties, and any and all records related to these actions. The data owner has final responsibility for the data and media, for its tracking, and for maintaining records of its movement.

- **COMPLIANCE:** The Information Security Office, will conduct random reviews, at least annually, on a representative sample of information systems to ensure compliance with this policy.

Departments may be guided in the disposal of equipment and media by the procedures outlined in the HOP, [Section 6.3.3](#), “Deletion of State Property” and [Section 6.3.4](#), “Changes and Reporting”.

At a minimum, when destroying, repurposing or transporting electronic media, the methods must comply with the [Media Control \(Accountability\) Security Standard](#) and the [Media Control \(Data Destruction\) Security Standard](#). The standards, as well as other security standards and guidelines pertaining to information security policies, may be found under Information Security on the Information Management and Services Web site: <http://ims.uthscsa.edu/policies.aspx>.

Accountability

Violations of this policy are subject to disciplinary action as described in the HOP, [Section 2.1.2](#), “*Handbook of Operating Procedures*”.
