



**The Division of Information Technology
University Information Security Standards**

**NIST CONTROL FAMILY
IDENTIFICATION AND AUTHENTICATION CONTROLS**

CONTROL NUMBER	CONTROL NAME	PRIORITY	REVIEW DATE
MP-6	Media Sanitization	P1	07/22/2017

I. STATEMENT

WTAMU sanitizes information system media prior to disposal, release out of University control, or release for reuse using approved and reliable sanitization techniques and procedures in accordance with applicable federal and organizational standards and policies; and employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

II. APPLICABILITY

This Control applies to all West Texas A&M network information resources. The intended audience for this Control includes all information resource owners, custodians, and users of information resources.

III. IMPLEMENTATION

Prior to the sale or transfer of data processing equipment to other than another Texas state agency or agent of the state, state organizations shall assess whether to remove data from any associated storage device. Electronic state records shall be destroyed in accordance with §441.185, Government Code. If the record retention period applicable for an electronic state record has not expired at the time the record is removed from data process equipment, the state agency shall retain a hard copy or other electronic copy of the record for the required retention period.

If it is possible that restricted personal information, confidential information, mission critical information, intellectual property, or licensed software is contained on the storage device, the storage device should be sanitized or the storage device should be removed and destroyed. Additional information on sanitization tools and methods of destruction (that comply with the Department of Defense 5220.22-M standard) are

provided in the “Sale or Transfer of Computers and Software” guidelines available at <http://www.dir.texas.gov>.