[Minor revision: June 21, 2018]

Angelo State University
Operating Policy and Procedure

OP 44.11: Media Protection

DATE: June 21, 2018

PURPOSE: The purpose of this policy is to define information security controls around media protection.

REVIEW: This OP will be reviewed in July every five years, or as needed, by the chief information officer and appropriate personnel with recommended revisions forwarded through the vice president for finance and administration to the president by August 15 of the same year.

POLICY/PROCEDURE

1. Definition

ASU defines technical policy terms in the information technology glossary.

2. Media Protection Policy and Procedures
Authority-DIR Controls Catalog (CC): MP-1

a. ASU must securely use, store and transport storage media containing sensitive information.

b. ASU must ensure university processes to secure sensitive information are effective.

3. Media Access
Authority- DIR CC: MP-2

a. ASU must ensure access to media is allowed only to authorized individuals.

4. Media Sanitization
Authority-DIR CC: MP-6

a. Before disposal or transfer, ASU must ensure removable media that contains sensitive information is securely erased or destroyed in a manner that ensures the information cannot be recovered or reconstructed. Additional information on sanitization tools and methods of destruction is available from DIR.

b. Electronic media (e.g., internal to computers, MFPs, and removable media) are either shredded or securely erased with tools approved by the ISO.

c. ASU must securely shred hard copies of sensitive information before disposal.

d. ASU must keep documentation of erasure or destruction that describes the process and sanitization tools used to remove the information or destroy the media, and includes the following:

   (1) Date of erasure or destruction;

   (2) Description of items and serial numbers;

   (3) Inventory numbers;

   (4) Process and sanitization tools used; and

   (5) The name and address of the organization the equipment was transferred to, if transferred.

e. ASU details records retention requirements in OP 02.07 and in the ASU Records Retentions Schedule.

f. When destroying storage media, ASU will transfer data required to be retained based on established records retention requirements in OP 02.07 and in the ASU Records Retentions Schedule.

5. Media Use
Authority-DIR CC: MP-7

a. ASU must adopt controls to safeguard university information in business office environments and on systems/devices/hard copy including, but not limited, to physically securing the media on which the university information is stored, encrypting sensitive information and handling/storage procedures for printed copies.

b. ASU should encrypt or physically secure sensitive information on removable media unless compensating controls are used.

c. ASU must restrict the use of mobile devices based on documented risk management decisions (see data classification standard).