[New policy: January 5, 2018]

Angelo State University
Operating Policy and Procedure

OP 44.20: Information Privacy and Protection

DATE: January 5, 2018

PURPOSE: The purpose of this policy is to define information security controls around information privacy and 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. Authority to Collect
Authority-DIR Controls Catalog (CC): AP-1

a. Information owners must establish procedures to ensure sensitive information is collected only when permitted by law or regulation.

b. Information owners must annually re-authorize information systems to contain sensitive information.

3. Inventory of Personally Identifiable Information
Authority- DIR CC: SE-1

a. Information owners must create and maintain an inventory of information considered sensitive and on which information systems this information is stored.

b. Information owners must provide, at least annually, updated sensitive information inventory and system list to custodians and ISO.

4. Privacy Notice
Authority-DIR CC: TR-1

a. ASU must provide all information requested as part of a formal open records request (see OP 01.02) except where prohibited by regulatory requirement.

b. ASU must use university held information only to conduct university business or as needed to operate and secure university information systems.

c. Employees, contractors, vendors, and affiliates of the university must safeguard the privacy and security of any information owned by or entrusted to the university.

d. Before sharing aggregated information, ASU must remove information that identifies individuals to prevent loss of individual privacy.

e. As part of security incident investigations, users may be asked to provide access to personally owned devices that were used to store or process university information.

f. ASU must ensure grades and other pieces of sensitive information will not be publicly posted or displayed in a manner where the Campus ID (CID) identifies the individual associated with the information.

g. Except where required by law, ASU must not require students to provide Social Security Number.

5. Internal Use
Authority-DIR CC: UL-1

a. ASU must use sensitive information only for authorized purposes.

b. Prior to sharing university held sensitive information, users must ensure any persons to whom they are providing such information are authorized to receive such information.

c. ASU must identify, document, and protect, in its entirety, any information file or record containing any confidential information.

d. ASU must protect the confidentiality of Category 1 and 1a information held by the university.

e. ASU must configure information systems so that they do not display Category 1 information unless required by the business process, where possible.

6. Information Sharing with Third Parties
Authority-DIR CC: UL-2

a. ASU must use procedural limitations, contractual obligations and statutory requirements to ensure that sensitive information shared with third parties is protected.