[New policy: January 5, 2018]

Angelo State University
Operating Policy and Procedure

OP 44.01: Acceptable Use Policy

DATE: January 5, 2018

PURPOSE: The purpose of this policy is to define requirements for the use of university information systems by all users.

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. Acceptable Use
Authority-DIR Controls Catalog (CC): PL-4

a. Users must act ethically and within the law when using university information and information systems.

b. Users must use university information systems only for university business and only as authorized by the information owner.

c. Users should use university information systems only in ways that benefit the university, ensure compliance with statutory requirements, are cost-effective, and enhance the reputation of the university.

d. Users are responsible for all actions taken using their university-issued accounts (or other methods of access). Users must not share passwords or other means of access.

e. By using university information systems, users consent to monitoring, logging and reporting on their use of university systems.

f. Users must use only university approved methods and technology to connect to the university's network and information systems.

g. Users must not use or disclose sensitive information, or data that is otherwise confidential or restricted, without appropriate authorization.

h. Users are required to report any weaknesses in security controls, incidents of misuse, and violations of university information technology operating and security policies to the Office of Information Technology.

i. Users must not purposely engage in activity that may harass, threaten, intimidate, endanger, or abuse others; degrade the performance of information systems; deprive an authorized user access to a university resource; obtain resources beyond those allocated; or circumvent technology security measures.

j. Users must not allow incidental personal use of university information systems to result in any embarrassment or non-trivial cost to the university.