[Minor revision: January 28, 2015]

Angelo State University
Operating Policy and Procedure

OP 44.01: **Security and Management of Protected Information**

DATE: January 28, 2015

PURPOSE: The purpose of this policy is to define Office of Information Technology policies for the management and security of protected information of faculty, staff, students and other constituents/affiliates of the university. This OP is not intended to apply to information that is subject to disclosure under state or federal laws and regulations.

REVIEW: This OP will be reviewed in January every three 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 February 15 of the same year.

POLICY/PROCEDURE

1. Overview

Data loss prevention policy and processes safeguard protected information for the entire campus. Protected information is expected to be used in accordance with applicable law or regulation and used responsibly, with courtesy, respect, and integrity. Anyone who has access to protected information on constituents/affiliates of the university (including but not limited to students, employees, alumni, vendors, contractors, etc.) must take reasonable and necessary steps to ensure privacy of such information.

2. Definition

a. Protected information is any information provided protection by law, regulation, or other legal means that mandates the methods, controls, processes, and/or procedures to afford such protection. This includes personally identifiable information (PII).

b. Personally identifiable information is any information that alone or in conjunction with other information identifies an individual, including Social Security numbers (SSN), driver's license numbers, military identification numbers, passport serial numbers, passwords/PINs, personal accounts, credit card numbers, protected health information, financial information, criminal history records, unpublished home addresses or phone numbers, biometric data, and any other information that is deemed confidential by law or university policy.

c. For other terms referred to in this document, please see the information technology glossary.

3. Security and Privacy of Protected Information

Authority-TAC: 202.75, 202.75.7.Z

a. Disclosure of protected information to unauthorized persons or entities is expressly prohibited.

b. Access to protected information must be granted through an appropriate approval process and revalidated on a regular basis.

c. Paper and electronic documents containing protected information must be secured during use and when not in use.

d. Electronic documents containing protected information must be stored only on systems configured with controls identified in the system's current risk assessment.

e. Any paper or electronic document (or media) containing protected information must be disposed of in a secure manner.

f. Controls must be adopted to safeguard protected information in business office environments and on systems/devices that contain such information. Safeguards may include, but are not limited, to physically securing the media on which the protected information is stored and encrypting the data.

g. Protected information should be encrypted while on disk or in storage. This includes storage on a computer, removable media, and file shares on centralized storage (e.g., P drives).

h. All applications that transmit protected information via a network must use encrypted connections for that transmission, or the information itself must be encrypted or otherwise protected while being transmitted.

i. Protected information must not be sent via e-mail unless the message is using university approved encryption or protected so that only the intended recipients can view the information. The information required to decrypt the message, such as the password, must not be included in the same message.

j. Protected information in document imaging systems (and other systems where digital images of protected information are permitted) should be protected (using controls such as access restrictions or redaction) so that view of protected information is available only by explicit user choice and available only to authorized users.

k. Grades and other pieces of protected information must not be publicly posted or displayed in a manner where either the Campus ID (CID) or SSN identifies the individual associated with the information.

4. Privacy and Protection of Social Security numbers

Authority-TAC: 202.75.7.R

a. Except where the university is required by law or regulation to collect an SSN, individuals must not be required to provide their SSN, verbally or in writing, at any point of service, nor will they be denied access to those services should they refuse to provide an SSN. However, individuals may volunteer their SSN if they wish to provide it as an alternate means of locating a record.

b. All university forms and documents that collect SSNs must use the appropriate language to indicate whether the request is voluntary or mandatory.

c. Except for those business processes in which the use of SSN is required by law or regulation, systems should be evaluated annually to determine if use of SSNs is still necessary. Steps should be taken to ensure that the SSN is not used as the primary key, except where absolutely necessary.

5. Incident Management

Authority-TAC: 202.71, 202.75.7.J

a. All security breaches of information systems containing protected information must be reported to the Information Security Office.

b. The university must disclose, in accordance with applicable federal or state law, incidents involving information resources containing protected information it maintains to information owners and any person whose protected information was, or is reasonably believed to have been, exposed or released without authorization.

   Disclosure must be made as quickly as possible upon the discovery or receipt of notification of the incident while meeting the legal requirements for handling of evidence and taking into consideration:

   (1) The time necessary to determine the scope of the incident and restore the reasonable integrity of operations; and

   (2) Any request of a law enforcement agency that determines that the notification will impede a criminal investigation. If so, notification must be made as soon as the law enforcement agency determines and notifies the Information Security Office of its determination that it will not compromise the law enforcement investigation.

6. Project Management

Authority-TAC: 202.75.6.B

a. For any project requiring protected information, the sponsoring department chair and/or the corresponding vice president must provide a signed affirmation that the use of protected information is required as part of the business process.

b. For any existing system, the Information Security Office must be informed of any changes to the system that may impact the system's risk profile.

c. The Information Security Office will determine whether additional review of technology projects is required.

7. New System Design
Authority-TAC: 202.75.6.B

a. The new system must use SSNs only if there is a clearly documented business need approved by the appropriate director or department chair.

b. The new system must use the SSN only as a data element or alternate key to a database and not as a primary key to a database.

c. The new system must not display SSNs visually (such as on monitors, printed forms, system outputs) unless required by business process.

d. New name and directory systems must be capable of being indexed or keyed on the CID, once it is assigned, not other protected information such as SSN.

8. Risk Assessments
Authority-TAC: 202.72.a.1

a. Systems that contain protected information must be classified as high risk for the purposes of risk assessments. These systems are required to be assessed annually.

9. Third party agreements
Authority-TAC: 202.75.7.X

a. Sharing of protected information with third parties is prohibited, except where there is a business need for the use of protected information by the third party and:

(1) The use is required or permitted by law; or

(2) The consent of the individual(s) identified by the protected information has been obtained.

10. Disposition of Protected Information
Authority-TAC: 202.78

a. Before disposal, removable media that contain protected information must be securely erased or destroyed in a manner that ensures the information cannot be recovered or reconstructed. Documentation of erasure or destruction must be kept and must describe the process and sanitization tools used to remove the data or method of destruction.

b. Printed documents containing protected information must be securely disposed of by a method that ensures that the information they contain cannot be recovered or reconstructed.

11. Office Environment
Authority-TAC: 202.75.7.R

a. Protected information displayed on computer monitors or other forms of output must not be visible to unauthorized viewers.

b. Information systems used as primary storage for protected information must not be physically accessible by anyone other than authorized users.

c. Individuals should not remove any media containing protected information from the university's facilities unless such removal is authorized by the data owner or appropriate controls are in place to secure the data.

d. Printers and other output devices, such as fax machines, to which protected information is sent should not be located in public areas, and if they are, must be attended at all times during which any protected information is being processed. Printed documents with protected information must be placed only in a secured area.

12. Training

a. HIPPA – All university employees required to handle or process protected health information will complete training on protected health information within 60 days of initial hire and annually thereafter each calendar year.

(1) Training will include pertinent points of applicable state and federal law.

(2) Employee must verify completion of training.

(3) The university will maintain verification of employee completion of training.

b. PCI DSS – All university employees required to handle or process credit card cardholder data will complete training on the secure handling of credit card cardholder data within 60 days of gaining access to the information and annually thereafter each calendar year.

(1) Training will include pertinent points of applicable policy and law.

(2) Employee must verify completion of training.

(3) The university will maintain verification of employee completion training.

13. Disciplinary Action

Violation of this policy may result in disciplinary action leading to or including termination for employees; termination of employment relations in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of access to Angelo State University information resources, and civil or criminal prosecution.