3.9.2

Student Affairs and Services: Student records

The institution protects the security, confidentiality, and integrity of student records and maintains security measures to protect and back up data.

Judgment

☑ Compliant ☐ Non-Compliant ☐ Not Applicable

Narrative

Note: Text for all linked documents below can be increased/decreased for ease of reading by pressing your keyboard's Ctrl key while rotating the mouse wheel.

Angelo State University defines and implements policies and procedures to protect the security, confidentiality, and integrity of student records and to ensure that special security measures are in place to protect and back up data.

CONFIDENTIALITY OF STUDENT RECORDS

The Family Educational Rights and Privacy Act (FERPA) governs access to and confidentiality of student records. Except as noted in FERPA, ASU will disclose information from a Student's Education Records only with the written consent of the student (Student Waiver to Release Education Information).

ACCESS TO AND INTEGRITY OF STUDENT RECORDS

ASU limits access to student records to protect student confidentiality and to ensure the integrity of the records.

ASU students are notified of their rights under FERPA in the ASU Student Handbook, which outlines the procedures students are to follow when requesting access to or amendment of their records. The handbook also includes information regarding the principal locations for student education records and the corresponding Records Custodians. As explained in the handbook, FERPA grants students the right to inspect and review their own educational records within 45 days of the day ASU receives a request for access. Students must submit to the registrar, dean, head of the academic department, or other appropriate official written requests that identify the record(s) they wish to inspect. The university official will arrange for access and notify the student of the time and place where the records may be inspected. If the records are not maintained by the university official to whom the request was submitted, that official will advise the student of the correct official to whom the request should be addressed. A student who believes that his or her Education Records are inaccurate or misleading, or that the records violate his or her privacy rights, is given the right to request an amendment to the record(s) that the student believes are inaccurate or misleading. In that situation, the student must submit a written request regarding the questionable item to the Records Custodian (ASU Student Handbook 2011–2012, pdf pp. 9–12).

ASU employees are granted access to student records on a need-to-know basis in accordance with the disclosure and access policies identified in ASU OP 44.00, Information Technology Operating and Security Policy. Electronic student records are maintained in Banner, an integrated online student information system that includes admissions, student records, and financial aid information. Records in Banner are protected by a comprehensive, password-driven security system, and each individual requesting access to Banner must first sign a Banner Request for Access Form indicating agreement with the compliance statement, conditions, and terms outlined on the form. The form includes information on FERPA, compliance expectations, and consequences for violation. Requests to access the system are directed to the ASU Office of Information Technology. This office notifies the ASU Office of the Registrar that a request for access to Banner has been made, and the registrar evaluates the request, determines whether access should be granted, and assigns the appropriate access level, if any. Levels of access, which include view-only and update, are assigned based on employee roles. For example, the level of access granted to teaching faculty and their designated staff allows them to enter grades directly into Banner. If a faculty member or designated staff person wishes to change a grade after the final grade has been posted, however, he or she must complete a Change of Grade form and submit the form to the Office of the Registrar. A member of the registrar's staff then enters the grade change into Banner. Data custodians, including the registrar, are required to review security permissions within Banner at least annually.

DISSEMINATION AND IMPLEMENTATION OF STUDENT RECORDS POLICIES AND PROCEDURES

Students are notified of their FERPA rights during orientation and annually thereafter through the student handbook (ASU Student Handbook 2011–2012,pdf pp. 9–12). FERPA rights are posted on the ASU website (FERPA Right #1; FERPA Right #2; FERPA Right #3; FERPA Right #4), and links to this information, as well as to the Student Waiver to Release Education Information, are available through the Student Services tab of the student portal. The student handbook and ASU OP 44.00, Information Technology Operating and Security Policy/Procedures, are also posted on the ASU website. When students or employees change their password via the change password web page, they are required to check the box indicating that they agree to abide by ASU information security policies as defined in ASU OP 44.00. If a student believes that ASU has failed to comply with the requirements of FERPA, the student has the right to file a complaint with the U.S. Department of Education, as described in the ASU Student Handbook 2011–2012, pdf p. 10.

To ensure that faculty and staff understand and carry out the commitments to confidentiality, integrity, and security of student academic records, ASU's department of Human Resources provides information regarding FERPA to all new employees (FERPA Compliance Statement). New hires are also required to sign the Employee Acknowledgement and Certification form stating that they have received the FERPA policy and that they understand how it pertains to their position with the university. Employees have access to the Faculty and Staff FERPA page of the ASU website that includes a resource page of frequently asked questions. An individual who uses or discloses information from a student's education record or allows access to an education record by another individual in violation of these regulations may be subject to disciplinary action, as outlined in ASU OP 44.00, Information Technology Operating and Security Policy (p.12, Section 25).

RETENTION AND DISPOSITION OF STUDENT RECORDS

Student records are maintained in accordance with ASU OP 44.01, Security and Management of Protected Information, OP 02.07 Records Retention, and the corresponding Records Retention Schedule. The retention schedule, which was prepared by ASU and approved by the State and Local Records Management Division of the Texas State Library, adheres to FERPA requirements and guidelines of the American Association of Collegiate Registrars and Admissions Officers.

The ASU Office of the Registrar is responsible for maintaining official student academic records. Academic records from 1928 through 1986 are maintained as hard copy originals with imaged backup, and academic records from 1986 through the present are maintained as electronic originals with electronic backup. The hard copy originals are kept behind locked doors in a fireproof vault on the first floor of the Hardeman building, which is located on the ASU campus. All electronic files, including the imaged backup files, are maintained on electronically and physically secured databases and servers.

SECURITY OF STUDENT RECORDS

As a state institution of higher education, ASU complies with information security standards established by the State of Texas in Title 1 of the Texas Administrative Code, Chapter 202, Subchapter C; see, for example, 1 TAC §202.70 (Security Standards Policy). To maintain compliance with these standards, the ASU Office of Information Technology maintains an Information Security Program. The key components of the ASU Information Security Program include risk assessment, technology tools that focus on security, processes to support these tools, and campus awareness and training initiatives. The security tools and processes provide a layered defense of ASU's information resources to minimize any single point of vulnerability. The security policies defined in ASU OP 44.00 are an outcome of the Information Security Program and require the responsible and secure use of information resources.

ASU's information systems have many physical and logical controls in place to protect the data and systems. The physical protections include using redundant hardware to prevent loss of availability or integrity due to hardware failure and restricting physical access to the data centers that house information systems to only those personnel who need to access the hardware. An example of a logical control is ASU's application of the principle of "least privilege" to the Banner system—only those with a business need to access the data are granted privileges to the system.

A regular backup schedule is in place to protect ASU's mission-critical data and systems. Backups are tested to ensure they can be used to restore systems in the case of hardware failure or disaster. Backups are sent off-site regularly so that a local disaster will not affect recovery of data. In the case of a larger incident, the ASU Office of Information Technology maintains and tests a disaster recovery plan that outlines a plan for restoring ASU's systems.