PRIVACY & SECURITY COMPLIANCE STATEMENT

The federal Family Educational Rights and Privacy Act (FERPA), Gramm Leach Bliley Act (GLBA), Fair and Accurate Transaction Act of 2003, and Stephen F. Austin State University's policies D-13, D-54, and C-60 govern the conduct of University employees with access to student and financial records. To ensure compliance, the University requires that employees be aware of federal and state law as well as University regulations that govern student and financial records. This statement clarifies the responsibilities of persons with access to student and financial records. All users sign this agreement as a condition of employment; others sign this statement as a condition of gaining access to the student and financial records systems.

Confidentiality. Security passwords must remain confidential. Employees must log off the Banner student system when leaving their computer workstation.

Education Records. Employees may access Banner student records only as required to perform assigned duties. Student records are confidential under law and cannot be disclosed without lawful authorization. Employees may not update their own record or that of a relative. Within the University, anyone whose designated responsibility requires access may use information from student records for appropriate job related functions relating to their educational need to know access to the student record data.

Financial Records. Employees may access Banner financial records only as required to perform assigned duties. Financial records are non-public, confidential records which should not be disclosed without lawful authorization. The use, access and security of financial records is governed by the University's Gramm Leach Bliley Act (D-54) and Identity Theft Prevention (C-60) policies, programs, and procedures.

Disclosure of Records. To respond to an inquiry for student records or information from outside the University, verify whether the student has checked the "Confidentiality" box on his/her records. This designation can be found on SPAPERS. A request for student records or information, such as a request for all seniors' mailing addresses, including requests for applicant information, from an organization or individual not affiliated with the University should be forwarded to the Office of the General Counsel for handling. A request for student records or information from an organization or individual within the University community, such as a student organization, should be forwarded for handling by the Office of Student Life. Unless explicitly suppressed by the student, the following "public" information may be released upon the receipt of a proper request for information:

> Student's name, all addresses including university issued e-mail address, all telephone number(s), major fields of study, academic classification, participation in officially recognized activities and sports, weight and height of members of athletic teams, dates of attendance and enrollment status, degrees and honors received, previous schools attended, photograph, and class rosters (not the student's class schedule).

All other information is private and may be released outside the University only in limited circumstances. Contact the Office of the General Counsel immediately for guidance before complying with a request for non-public information. No information on financial aid records may be released outside the University except as authorized or required by federal and state regulations. **Also, within the University, publishing of non-directory information, especially social security numbers and campus ID's, should be kept to an absolute minimum. (Publishing includes, but is not limited to, copies of the information for office or workgroup use, formal reports, and fact books.) Such publishing should be limited to within office or workgroup use. Identification numbers should never be published in documents intended for general consumption. Hard-copy documents should be kept in secured locations, and electronic files containing non-public information should not be kept on laptop hard-drives, flash drives, or other portable media devices.**

Staff granted access to Banner student institutional databases or batch files agree to:

- Comply with all data standards policies as presented in the Guidelines for Data Standards, Data Integrity and Security ;
- Comply with the Student Records (D-13), Gramm Leach Bliley Required Information Security (D-54), Identity Theft Prevention (C-60), and all other applicable policies and procedures relating to the possession, security and transfer of student educational and financial records;
- Store information under secure conditions;
- Make every effort to ensure students' privacy;
- Destroy information when it is no longer needed in compliance with the University's record retention policy;
- Use information only as described in the request for data or access to institutional database files;
- Release information to a third party only if authorized approval is given and in accordance with this Compliance Statement, University policy, and state and/or federal law;
- Never represent summary data from files as "official" University data.

Violations. Violation of Federal law or University policy constitutes grounds for rescinding access to Banner records or imposing disciplinary action, up to and including dismissal. Violations include the following offenses and any other comparable action:

- Not adhering to data standards guidelines as presented in the Guidelines for Data Standards, Data Integrity and Security
- Not complying with the Student Records (D-13), Gramm Leach Bliley Required Information Security (D-54), Identity Theft Prevention (C-60), and all other applicable policies and procedures relating to the possession, security and transfer of student educational and financial records;
- Releasing public information about a student whose information was requested on the basis of non-public information (e.g., names of all international students, name of all students with a GPA lower than 2.0);
- Altering a student's record without appropriate supporting documentation/authorization.
- Accessing a student record outside of your assigned duties;
- Releasing suppressed or non-public/directory information without authorization;
- Publicly discussing a student's record in a way that might personally identify that student;
- Sharing computer security passwords.

I have read this compliance statement and agree to the conditions and terms outlined herein.

Name (Please Print)	Department
Campus ID Number (CID)	Date
Signature	Title

Approved by General Counsel 07/09