

**Safeguarding Student Financial
Information Policy
Fort Hays State University**

Posted Revision 06-23-04

General - Fort Hays State University ("FHSU") has adopted this policy in compliance with the Gramm-Leach-Bliley Act (GLB Act, Sec 16CFR Part 314). This policy will be reviewed and adjusted as necessary, at least on an annual basis. The FHSU Internal Compliance Coordinator will report to the Vice President of Administration and Finance in written form at least annually or more frequently if material events warrant.

Providing Safeguarding Policy Notices - FHSU will provide safeguarding student information policy notices as required by the GLB Act. Students will be sent initial safeguarding student information policy notices to their permanent addresses. Thereafter, students will be sent safeguarding student information policy notices at least annually. New students will receive safeguarding student information policy notices at the time of application or approval of services. Safeguarding student information policy notices will be provided in a form that the student may access at a later time.

Collection of Student Information - FHSU collects information about students in many ways. Information is provided by students to FHSU on admission applications, financial aid applications, and through a variety of other forms and services. FHSU also receives information when processing student transactions such as clearing checks, ACH transfers, debit transactions, and more. Students also provide information in response to questions posed by FHSU or in their correspondence to FHSU. All nonpublic personal information collected is subject to the confidentiality provisions of this policy.

Confidentiality and Security of Student Information - FHSU will undertake reasonable measures to protect the confidentiality and security of student information. Physical security of documents, restricted access to information, and proper handling of information form the basis of FHSU's procedures. (1) FHSU employees will verify students' identity before releasing information or processing transactions for students. (2) FHSU employees will also maintain control and security of documents that contain student information. After processing, documents with nonpublic personal information will be properly filed or discarded. (3) FHSU employees are allowed access to students' information as needed to fulfill students' requests or conduct FHSU business as may be appropriate. (4) FHSU maintains physical, electronic, and procedural safeguards to protect student information.

Application to Former Students - FHSU's disclosure policies are applied to former students in the same manner as they are to current students.

NPI collected by FHSU - FHSU collects only nonpublic personal information (NPI) that is needed for the transaction or service a student requests. FHSU may collect this information from the following sources: (1) Information FHSU receives from a student's application or other forms (2) Information about a student's prior transactions with FHSU or others (3) Information FHSU receives from a consumer reporting agency, if any.

Types of NPI FHSU Discloses and to Whom FHSU Discloses NPI - Although FHSU does not generally disclose a student's nonpublic personal information to outside parties, we may disclose any of the nonpublic personal information we collect under the following circumstances: (1) When a student asks or gives FHSU permission to do so; (2) In furtherance of the transaction or service a student requests; (3) As otherwise permitted or required by law. For example, a disclosure made to an entity to which a student has identified FHSU as a credit reference if such disclosure is limited to information related to the student's specific transactions or experiences with FHSU. (4) To Third Party Affiliates. For example, FHSU may disclose a student's nonpublic personal information to its agents, but only to the extent necessary to further the transaction or service, such as a collection agency or Credit Bureau.

Pretext Calling - FHSU prohibits its employees from obtaining, attempting to obtain, or causing to be disclosed, student financial information relative to another person by use of false or fraudulent practices. These practices include: (1) Making a false statement to an employee of FHSU, (2) Making a false statement to a student of FHSU, or (3) Providing, to an employee of FHSU, a document that a person knows is false, stolen, fraudulently obtained, or contains a false representation. Inquiries made to FHSU shall require the verification of the identity of the requesting party, a determination of the reasons information is being requested, and a determination of the authorization of the student to disclose the information. Authorization by the student may include the issuance of a check, an application for credit, an express authorization for verification, or other means that may be deemed reasonable.

Training - FHSU employees with access to student financial information defined by the GLB Act will participate in training on safeguarding student information. This issue will be covered as part of employee orientation and as needed in departmental meetings. Student privacy issues, FHSU's privacy policy, and appropriate procedures will be reviewed annually with all employees. Applicable employees are trained to respect students' privacy through compliance with FHSU's policies and procedures. Failure to comply will subject employees to disciplinary action.

Security Statement - FHSU is committed to ensure the confidentiality of students' online transactions. FHSU banking products incorporate designed-in security features for safeguarding student accounts and the information students transmit to FHSU during a session.

Security Features

Data Encryption - For student protection, FHSU requires 128-bit Secured Socket Layer (SSL) strong encryption during students' online sessions with Student Web Services. Encryption is a sophisticated way of scrambling all information transmitted online before it leaves a student's computer, so that all information, including passwords and online bill payments are completely unreadable by unauthorized third parties. No transactional information will be transmitted without first being encrypted.

FHSU requires that a student's web browser support 128-bit encryption because it is more effective than 40-bit encryption. While 40-bit encryption might be fine for low risk transactions, it is not adequate for protecting financial transactions. When students supply data via the Internet, it is encrypted before it travels across the world-wide-web. FHSU decodes and processes the data at our end of the transaction process. When FHSU provides data to students, the data is encrypted by FHSU and sent to the student. When the student receives the data or information, the student's browser decodes the information and displays it to them. Students can ensure that online information is encrypted in Internet Explorer or Netscape if the small key or lock at the bottom left-hand or right-hand corner of their screen is latched.

Approved Browsers - Windows 95/98/NT/XP - Microsoft Internet Explorer v 4.01, 5.0, 5.01(AOL5), 128-bit; Windows 95/98/NT/XP - Netscape Navigator v 4.08, 128-bit; Windows 95/98/NT/XP - Netscape Communicator v 4.51, 4.61, 4.7, 4.72, 128-bit; Macintosh OS 8.x - Microsoft Internet Explorer v 4.01, 4.5.1, 128-bit; Macintosh OS 8.x - Netscape Navigator v 4.06, 128-bit; Macintosh OS 8.x - Netscape Communicator v 4.7, 128-bit.

Individualized Password - When a student enrolls, the student is provided with a User Name and initial online password. Students may change the password as often as they wish. The first time the student logs in the student will be required to change passwords. Every time the student begins an online session after the initial log in, the student will need to enter the student's User Name and password to enter the secure area of the FHSU website.

Timed Logoff - If the student forgets to logoff, FHSU will log the student off by terminating their FHSU account session after a certain length of time. The session time will be determined centrally. This built-in safeguard protects student account information from unauthorized access in the event the student is called away from the computer during an online session, or in the event the student forgets to logoff at the conclusion of the student's session.

Database Server Security - The mainframe database server, the data warehouse, and the PowerFunds financial aid server are all protected by a private IP address so that they are invisible to those seeking unwarranted access over the Internet. The Sungard database server has a firewall to prevent unwarranted access from the Internet. Access to that server over the Internet can only be accomplished for authorized users by using a special VPN.

E-Mail Security - Students use the university e-mail system (their Scatcat e-mail address) for official transactions. When students access their e-mail using the web, their e-mail is also encrypted at the 128-bit level of encryption. This is the typical way students access their e-mail. If they use POP-3 access, they can also encrypt it at the 128-bit level.

Student Responsibilities - Each of the foregoing security features is designed to protect confidentiality of a student's online transactions and account information. The student is also responsible for adhering to the following secure practices: (1) NEVER reveal logon ID or password to anyone, (2) NEVER leave PC unattended during a session, (3) Be sure to LOG OFF completed sessions before visiting other web sites, (4) If the browser cannot be closed after a banking session, be sure to delete the temporary files stored by the browser on the local hard drive by consulting the browser Help on how to do this, (5) Report known instances of unauthorized account access to FHSU within the required timeframe, (6) NEVER use email to transmit any personal, business, financial or account information because messages sent in this manner are not encrypted., (7) Use the encryption features of a browser where an upgrade may be required of the browser to 128-bit encryption.

If a student has any questions regarding the security of their online transactions, please call the Computing & Telecommunication Center (785-628-4487).