

# **SAFEGUARDING STUDENT FINANCIAL INFORMATION**

## **POLICY – SECURITY**

### **FORT HAYS STATE UNIVERSITY**

**Effective 05/23/03**

#### **Security Statement**

Fort Hays State University ("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

Microsoft Internet Explorer v 4.01, 5.0, 5.01(AOL5)

128-bit

Windows 95/98/NT

Netscape Navigator v 4.08

128-bit

Windows 95/98/NT

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 the student may 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 (in the SunGard system). 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 PowerFaids 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 the 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 for official transactions (their FHSU e-mail address). 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.
  - NEVER reveal logon ID or password to anyone.
  - NEVER leave PC unattended during a session.
  - Be sure to LOG OFF completed sessions before visiting other web sites.
  - 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. Consult the browser Help on how to do this.
  - Report known instances of unauthorized account access to FHSU within the required timeframe.
  - NEVER use e-mail to transmit any personal, business, financial or account information. Messages sent in this manner are not encrypted.
  - Use the encryption features of a browser. An upgrade may be required of the browser to 128-bit encryption.

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

*Approved by President's Cabinet 06/04/03*