Stockton University
Information Security Plan

I. Purpose

Federal Trade Commission (FTC) Regulation 16 CRT Part 314 requires financial institutions (including institution that participate in the processing of financial loans, such as colleges and universities) to have a security plan to protect the confidentiality and integrity of personal consumer information. The plan must document the security systems and/or measures it has established to secure the nonpublic financial information of its customers.

The purpose of this document is to reaffirm the safeguards that have been established by the University to secure its administrative information systems, which store, transmit, retrieve, process and dispose of nonpublic financial, confidential, personally identifiable, trusted or otherwise protected information, against unauthorized use, intrusion or other security risks. This document serves as the University's information security plan as required by FTC Regulation 16 CRT Part 314.

II. Information Systems

Information systems consist of the software, hardware and communication networks that are used to process, store, transmit, retrieve and dispose of data. Following are the administrative information systems that are used by the University for purposes relating to financial loan processing. These and other similar systems used by the University are subject to the FTC safeguarding rule:

University Financial Systems
Student Information System
Financial Records System
Financial Aid System and EdeXpress

External Financial Aid Processing Systems
ED Connect
FAFSA On The Web
Luareatte Loan Servicer
Citibank
Key Bank
Fleet Bank
Teri Loan
Nellie Mae

Federal Government Web Sites and Facilities including
COD Web Site
Enrollment and Financial Aid Data Clearing House Site
NSLDS Financial Aid Data Site
SAIG Reporting Site
FSA Information Site
US Dept of Education
Veterans Software Database
Monster FWS Database
IPADS Site

State of NJ Web Sites and Facilities including
HESAA Site for Grants/Loans/Scholarships
NJASFAA and NASFAA
Common Database Site

The following information systems contain data that may be nonpublic, financial, confidential, personally identifiable, trusted or otherwise protected. Access to these systems is therefore restricted. Authorization to access these systems or use the data stored in these systems is granted by a designated data custodian.

<table>
<thead>
<tr>
<th>SYSTEM</th>
<th>CUSTODIAN (Director or head of)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Banner Student Information System</td>
<td></td>
</tr>
<tr>
<td>Undergraduate Admissions</td>
<td>Admissions Office</td>
</tr>
<tr>
<td>Graduate Admissions</td>
<td>School of Graduate Studies</td>
</tr>
<tr>
<td>Shared Data</td>
<td>Student Records Office</td>
</tr>
<tr>
<td>Records and Registration</td>
<td>Student Records Office</td>
</tr>
<tr>
<td>Financial Aid</td>
<td>Financial Aid Office</td>
</tr>
<tr>
<td>Student Receivables</td>
<td>Bursar’s Office</td>
</tr>
<tr>
<td>Academic Advising</td>
<td>Advising Office</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Banner Human Resource System</td>
<td></td>
</tr>
<tr>
<td>Payroll</td>
<td>Payroll Office</td>
</tr>
<tr>
<td>Labor Distribution</td>
<td>Office of the Dir. of Budget</td>
</tr>
<tr>
<td>Personnel Records</td>
<td>Human Resources Office</td>
</tr>
<tr>
<td>Benefit Record</td>
<td>Human Resources Office</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Banner Alumni and Development System</td>
<td></td>
</tr>
<tr>
<td>Advancement Records</td>
<td>Alumni and Development</td>
</tr>
<tr>
<td>Alumni Records</td>
<td>Alumni and Development</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Banner Finance System</td>
<td></td>
</tr>
<tr>
<td>Financial Account</td>
<td>Office of the Dir. of Budget</td>
</tr>
<tr>
<td>Accounts Payable</td>
<td>Office of Accounts Payable</td>
</tr>
<tr>
<td>Purchasing</td>
<td>Purchasing Office</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>E – Mail Systems</td>
<td></td>
</tr>
<tr>
<td>Library Management System</td>
<td>Office of the Director of the Library</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>CBORD Board and Debit System</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bursar’s Office</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Central Stores</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Central Stores</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Academic facilities and systems</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Office of Computer Services</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Course Management systems</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Office of E-Learning</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Fixed Asset Inventory</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Office of the Controller</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Housing Management systems</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Office of Housing and Residential Life</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Facilities Maintenance systems</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Office of Plant Management</td>
</tr>
</tbody>
</table>

Information Security Plan 2 April 21, 2015
III. Safeguarding Information Systems

Following are the practices and security measures that have been established by the University to safeguard its administrative computing systems.

**Information Systems Control**

Nonpublic information (i.e., data that is confidential, personally identifiable, proprietary, trusted or otherwise protected information) obtained through University administrative software systems must be treated as confidential, and can only be used in connection with a person's job responsibilities.

Information obtained through the University's computerized administrative systems is the property of Stockton University and shall not be disclosed to persons outside of the University unless authorized by the designated data custodian, or to persons within the university unless such information is needed in their job assignments.

The disclosure of nonpublic student information is specifically governed by the Family Education Rights and Privacy Act and cannot be released to a third party without the written consent of the student. The disclosure of nonpublic financial information is specifically governed by the FTC regulation.

Requests to access the University's administrative software systems for the purpose of viewing, update and processing of data must be approved by the person who serves as custodian of the system. Users who have been granted access to systems must follow appropriate data control procedures to verify system integrity and accuracy of data.

**Data Control**

Data control procedures are used to verify that the integrity of data files has not been compromised as a result of batch or on-line processing.

It is the responsibility of on-line users who maintain institutional data to develop data entry procedures that minimize data entry error. Further, on-line users must develop appropriate data control procedures to assure accuracy and integrity of institutional data files.

It is the responsibility of any office conducting batch or on-line processing of institutional data files, particularly those which involve updating (i.e., changing, adding, or deleting) data, to establish and follow appropriate data control procedures. Data control procedures must at a minimum:

- Verify the reliability and integrity of data using sound, well-defined verification methods such as, for example, hashing or sampling against previously arrived at manual calculations or results. Additionally, processes that update data in mass should be run first with a "no update" option or should be tested in non-production environments.
- Provide thorough documentation regarding the procedures that employees must follow in processing data and verifying the correctness of processing.

**Data Backup**

As a safeguard against accidental data loss, data supporting the University's central administrative system (Banner) must be routinely backed up. Banner system data are backed up in real time to a
mirror site. Data on the mirror site is backed up to tape nightly and taken to a secured, off-site location. Other central administrative processing systems or servers supporting critical administrative functions must be backed up following each workday. Backup tapes or disks must provide for the recovery of data spanning a one-month period. Backup files must be stored in a secured off-site location or in a fireproof and secured vault. PCs, workstations and restricted use processors should be backed up on an as needed basis. As a standard practice, all files that are stored in the “My Documents” directory and its associated sub-directories on employee desktop computers are automatically backed up in real-time to a secure central storage facility.

Data Archive and Retention

A complete system back up of central processing systems or servers supporting critical administrative functions must be performed at the end of each calendar and fiscal year. Archive tapes must be retained indefinitely.

Security

Appropriate safeguards must be taken to assure the integrity and reliability of the University’s institutional data resources. Offices maintaining institutional data on PCs are responsible for establishing and following appropriate data security practices. All backup media containing confidential or sensitive data must be stored in a physically secured area or encrypted using a strong password or key. The Office of Computer and Telecommunication Services is responsible for safeguarding institutional data that resides on the University’s central computing facilities. Systems containing confidential or sensitive information must require users to authenticate themselves using industry accepted account and password authentication methods.

Account Security

Faculty and staff may have access to administrative computing accounts, as needed, in accordance with their job responsibilities. Computer accounts are requested in writing. All users are required to abide by the University’s Standards Concerning the Acceptable Use of Computing Facilities. These standards, which are posted on the University’s web site, address the acceptable usage of computing facilities and the responsibility of account holders for data confidentiality.

In accordance with the University’s Standards Concerning the Acceptable Use of Computing Facilities, only persons authorized by the Executive Director of Computer and Telecommunication Services may be granted computing accounts. Access to and use of administrative computing facilities may be granted to appropriate personnel by the Executive Director of Computer and Telecommunication Services provided the recognized custodian of the data for which access is requested has authorized such access and use.

The use of group or shared accounts should be avoided. Passwords for administrative computer accounts are automatically expired. Administrative computer accounts or accounts with system privilege or programmer accounts with direct access to administrative production systems must be changed at a minimum of every ninety days. Other administrative accounts must be changed every one hundred and eighty days.

Computer accounts that permit access to administrative or other protected data must be promptly disabled whenever account holders resign their position, retire or otherwise leave the University.

Network and System Security
Network systems must be designed to reasonably limit the risk of unauthorized access to administrative information systems. Additionally, appropriate safeguards must be in place to monitor network security and respond to potential attempts to breach security. For example, system logs must be enabled to report unauthorized access attempts and reviewed on a frequent basis (daily, when possible); CERT (Computer Emergency Response Team) or other similar bulletins must be monitored; reasonable security recommendations from software or system vendors must be promptly applied; employees accessing information systems containing confidential or sensitive information must use communication software that encrypts accounts and passwords; firewall and filter systems should be implemented, where appropriate.

Access restrictions are imposed on users who access the university’s computing facilities via the Internet. Users with privileged computer accounts (system administration accounts) or accounts that permit direct update access to administrative information systems must use a virtual private network (VPN) when accessing systems via the Internet. Faculty or staff requiring access to systems via a VPN must request access through the Office of Computer and Telecommunication Services. Access cannot be provided where in the judgment of the Executive Director of Computer and Telecommunication Services such access may compromise system security.

The transmission of confidential or sensitive data over the public Internet to web-based applications or servers must utilize trusted communications protocols, such as SSL or Secure FTP.

Administrative Applications Security

Banner, which is used to support the University’s administrative operations, provides for user account, on-line form, data element and data value security that is capable of restricting persons from updating or viewing of data base elements selectively. The Office of Computer and Telecommunication Services administers security for the University’s administrative computing systems, excluding the value-based security within the financial records and human resource systems, which are administered by the Office of Budget and Office of Human Resources, respectively.

Computer and Telecommunication Services maintains training, test and production (live) versions of administrative (Banner) software systems. Users are issued individual accounts to production versions of these systems. The use of shared accounts on production systems is not permitted. Programmers and other authorized Office of Computer and Telecommunication Services staff responsible for maintaining application software systems are granted on-line application access accounts with read only (inquiry) access to production system’s transactional data and read and write access to test and training systems. (Programmers and other authorized Office of Computer and Telecommunication Services staff may be granted limited access to production system data that are used to configure and control system processes). Computer & Telecommunication Services staff that are granted access to data must carefully observe the security standards and practices outlined in this document.

Access to administrative system’s source code, executables, command files and data files is strictly controlled. Users must be only permitted access to data through the on-line application system interface. User access at the operating system level is not permitted unless it is unavoidable and necessary to perform assigned job duties. User access at the database level is likewise prohibited. Programmers, operators or other technically qualified personnel assigned to a functional area may be given access to production, test and training files and programs at the operating systems or database level for the sole purpose of conducting their assigned duties. The custodian of the application system must be informed of any changes to production systems made by Computer & Telecommunication Services staff. Changes to source code, including patches supplied by the
vendor, must be fully tested by end-users in a non-production environment and approved by the
designated system custodian prior to being moved to a production system by Computer &
Telecommunication Services staff.

Integrity Assurance Controls

Following are examples of controls, which must be followed, to assure application system
integrity:

- Changes to programs or previously un-tested batch processes must be made on the test
  version of systems prior to their transfer to production systems.
- Acceptance tests must be satisfactorily performed prior to a system being moved to
  production.
- Users must develop testing data and testing acceptance procedures.

Separation of Responsibility

The following practices, which assure separation of duty, must be observed:

- All negotiable paper or electronic dongels (keys) used to produce negotiable documents
  must be stored, controlled, and accounted for by the designated system custodian.
- Producing and finalizing a negotiable document must also involve an office other than the
  office where negotiable paper is stored.
- All negotiable paper must be numbered and its use logged.
- All official documents, such as transcripts or diplomas, must be stored, controlled and
  accounted for by the designated system custodian.
- All official documents must be stamped with an official seal, which must be kept in a
  secured location.
- All runs involving negotiable paper must take place in a physically secured location during
  weekday shifts with at least two people present.
- Computer and Telecommunication Services personnel must not run update processes or
  change transactional data on production systems unless specifically directed to do so by the
  appropriate data custodian.
- All batch production runs must be requested by user offices and approved by data
  custodians.
- Changes to application systems may not occur without written user request and approval of
  data custodian.

Physical Security

The University's central computing resources are located in D130. Equipment and wiring which
support the University's communications networks are located throughout the campus in
communications and wiring closets. Access to these facilities is restricted to Computer and
Telecommunication Services staff, Plant Management and campus security personnel in the
conduct of their assigned duties, and others having a job related need who have also been
authorized by the Executive Director of Computer and Telecommunication Services or the VP for
Administration and Finance or the Provost.

Virus Protection
PCs on the University’s LAN that are connected to a computer network or available for public access or which share data via file upload or removable media are at risk of being infected by a computer virus. The University holds a site license to anti-virus software. All at risk systems must run anti-virus software at all times. Anti-virus software must be configured to automatically retrieve anti-virus software updates.

Use, Storage and Disposal of Confidential Materials

Printed materials that contain confidential or sensitive information must be properly filed. They must be stored in secured areas where access is limited to authorized personnel. Personnel that are granted access to confidential or sensitive information must take measures to guard against casual viewing by others. PC monitors must be shielded from public view. Care must be taken to prevent unauthorized persons from using the computer. Authorized personnel must, for example, signoff administrative applications or conceal and password protect their computer displays when they are away from their work area.

Printed copies of confidential or sensitive information must be handled by authorized personnel and kept in areas with restricted access. Additionally, printed materials must not be left in the open on attended desks for extended periods of time.

Materials and/or reports that contain confidential or sensitive information are to be disposed of in a manner that safeguards against unauthorized disclosure of information.

When computers are relocated for use within the University, confidential data must be deleted from disk and file systems. Computers that are transferred to Central Stores for auction, reuse or disposal must have their disk and file systems reformatted or purged.

Notebook computers, flash drives or removable hard drives acquired by the university for administrative purposes must be equipped and configured to automatically encrypt administrative data.

Payment Card Data Security

Offices processing credit and other payment cards through manual or automated means must fully comply with Payment Card Industry Data Security Standards. The automated processing of credit and other payment cards must be made through trusted, PCI-DSS and PA-DSS compliant, 3rd party payment processors. Cardholder data must not be stored locally in an electronic format. Additionally, cardholder data must not be transmitted over non-secured channels. The transmission of cardholder data via email or other messaging applications is not permitted. Cardholder data may only be stored in hard copy and hard copy documents must be classified as confidential and physically secured. Further, the moving and transport of hard copy documents containing cardholder data must be authorized by management and transported securely in a manner that provides for tracking of data during transport. Media containing cardholder data must be properly destroyed when it is no longer needed for business or legal reasons.

Employees who have administrative responsibility for credit and other payment card processing may be granted access to 3rd party payment processing sites to oversee payment processing and view remotely stored cardholder data. These employees are required to use a restricted purpose, secure computer when accessing the 3rd party gateway processing sites. The computers used to access 3rd party payment sites must not be equipped with a wireless interface, must automatically apply security and virus protection updates, must log security related events, must communicate using strong cryptography and security protocols (e.g. secure sockets), must be located in a protected local area subnet and be restricted at a firewall from unauthorized access.
* According to PCI standards: “At a minimum, cardholder data contains the full PAN [Primary Account Number, or credit card number]. Cardholder data may also appear in the form of the full PAN plus any of the following: Cardholder name, Expiration date, Service Code.”

III. Responding to Information System Security Threats

Following are measures that should be taken to protect against security threats

Examine Security Logs - The Office of Computer & Telecommunication Services and other offices maintaining computing systems where information that is protected by regulation or law is stored must, were practical, enable operating system features that report upon security threats. The system security reports and logs must be examined at least weekly.

Evaluate Suspected Security Breaches - Suspected security breaches must be reported to the University’s officer in charge of risk management. The officer in charge of risk management is responsible for the thorough evaluation of suspected security breaches that may have disclosed protected information. The Office of Computer & Telecommunication Services will assist the officer in charge of risk management in the evaluation.

Notify Effected Persons - In cases where the officer in charge of risk management affirms that non-public information, as defined under FTC Regulation 16 CRT Part 314, has been disclosed to an unauthorized party the University must promptly notify any effected person.

Conduct Periodic Security Review – On an annual basis the University’s network and administrative systems should be tested to determine whether they are meeting industry standards for access control and security.