

STOCKTON UNIVERSITY

INFORMATION SECURITY PLAN



Information Security Plan	2
1. Information Systems	3
2. Data: Classification, Storage and Retention, Transmission & Destruction	5
a. Safeguarding Personally Identifiable and Confidential Information	6
b. Data Classification	8
c. Data Storage and Retention	11
d. Data Transmission	13
e. Data Destruction	14
3. Safeguarding Information Systems	15
4. Responding to Information System Security Threats	21
5. Appendix	25

Information Security Plan

Statement of 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 security plans and practices 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 foundation of the University information security program as required by FTC Regulation 16 CRT Part 314.

The University's Information Security Plan applies to any record containing nonpublic financial information about a student, employee, or third party who has a relationship with the University, whether the record is in paper, electronic, or other form, that is handled or maintained by or on behalf of the University or affiliated organizations. The Chief Information Officer, in consultation with the Chief Financial Officer and General Counsel, are responsible for reviewing and revising the Information Security Plan.



Information Security Plan Sections

- 1. Information Systems
- 2. Data: Classification, Storage and Retention, Transmission & Destruction
 - a. Safeguarding Personally Identifiable and Confidential Information
 - b. Data Classification
 - c. Data Storage and Retention
 - d. Data Transmission
 - e. Data Destruction
- 3. Safeguarding Information Systems
- 4. Responding to Information System Security Threats
- 5. Appendix

1. Information Systems

Information Systems

i 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 Sites and Facilities

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 New Jersey Sites and Facilities

HESAA Site for Grants/Loans/Scholarships
NJASFAA and NASFAA
Common Database Site

Restricted Access

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.

Information System Custodians**Banner Student Information Systems**

System	Custodian
Undergraduate Admissions	Admissions Office
Graduate Admissions	School of Graduate Studies
Shared Data	Student Records Office
Records and Registration	Student Records Office
Financial Aid	Financial Aid Office
Student Receivables	Bursar's Office
Academic Advising	Advising Office

Banner Human Resource Systems

System	Custodian
Payroll	Payroll Office
Labor Distribution	Office of the Dir. of Budget
Personnel Records	Human Resources Office
Benefit Record	Human Resources Office

Banner Alumni and Development Systems

System	Custodian
Advancement Records	Alumni and Development
Alumni Records	Alumni and Development

Banner Finance Systems

System	Custodian
Financial Account	Office of the Dir. of Budget
Accounts Payable	Office of Accounts Payable
Purchasing	Purchasing Office

Computing Systems

System	Custodian
Email Systems	Information Technology Services
Library Management System	Office of the Director of the Library
CBORD Board and Debit System	Bursar's Office
Central Stores	Central Stores
Academic Facilities and Systems	Information Technology Services
Course Management Systems	Information Technology Services
Fixed Asset Inventory	Office of the Controller
Housing Management Systems	Office of Housing and Residential Life
Facilities Maintenance Systems	Office of Plant Management

2. Data: Classification, Storage and Retention, Transmission & Destruction

i The purpose of this section is to highlight the different aspects of data management 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 and otherwise protected information. Each section further analyzes all aspects of data management such as data classification, retention, transmission, and destruction.

Data: Classification, Storage, Retention, Transmission & Destruction Sections

- [a. Safeguarding Personally Identifiable and Confidential Information](#)
- [b. Data Classification](#)
- [c. Data Storage and Retention](#)
- [d. Data Transmission](#)
- [e. Data Destruction](#)

a. Safeguarding Personally Identifiable and Confidential Information

Safeguarding Personally Identifiable and Confidential Information

For the purposes set forth in this document, the University's computing and communication facilities include all computing, video, data and telecommunication hardware and software systems owned, leased, or granted to the university.

Personally Identifiable Information

Personally Identifiable Information (PII) refers to any data that identifies or can be used to identify, contact, or locate the person to whom such information pertains. This includes data that is used in a way that is personally identifiable, including linking it with identifiable information from other sources, or from which other personally identifiable information can easily be derived, including, but not limited to, name, address, phone number, fax number, external email address, financial profiles, social security number, drivers license number or identification number, credit card information, alien registration number, passport number, employer or taxpayer identification number, student identification number, and Internet Protocol address or routing code.



Note Regarding Personally Identifiable Information

Access to administrative data may be granted to individuals for the purpose of enabling them to fulfill specific job duties or contracted services or in furtherance of legitimate university business. Custodianship of data that is maintained on the University's primary administrative information systems is detailed below.

Definitions

Administrative Data

Administrative data refers to any data that are collected, maintained and used on administrative information systems that support the operations of the University.

Confidential Data

Confidential data refers to any data pertaining to individuals or the University that is sensitive, private, or of a personal nature, or data that is protected under a confidentiality agreement, regulation, law, or University procedure.

Institutional Data

The use of the term "*institutional data*" hereafter within this document is meant to refer to all personally identifiable information, administrative data or confidential data residing or accessible through the University's computing and communication facilities, or any facility, service or device (privately owned, leased, or granted) containing data created by the University or entrusted to the University.

Guidelines for Safeguarding Personally Identifiable and Confidential Information

Authorized use of and access to the University's computing and communication facilities is intended and permitted solely to support the legitimate educational, administrative and missioncentered programs of the institution. Authorization for the use of and/or access to the University's computing and communication facilities is granted by the Chief Information Officer and the Director or supervisor of the organizational unit that is the recognized steward and custodian of the data for which access is requested.

The University will take the following steps with respect to its internal operating procedures to protect identifying information:

- Ensure the University's website is secure or provide clear notice that the website is not secure;
- Ensure complete and secure destruction of paper documents and computer files containing identifying information when such documents or files are no longer needed;
- Ensure that office computers with access to Covered Account information are password protected;
- Avoid use of social security numbers and allow access to social security numbers to very limited number of staff that have been approved by the Program Administrator;
- Ensure computer virus protection is up to date;
- Require and keep only the kind of information that is necessary for University purposes.
- Require all notebook computers, flash drives or removable disk drives acquired by the University for administrative purposes to be equipped and configured to automatically encrypt administrative data.

b. Data Classification

Data Classification

i Information may be classified when needed into one of the following three levels:

Level 1 - Confidential

Level 2 - Private

Level 3 - General

The three levels described below are meant to be illustrative, and the list of types of data contained below is not exhaustive.

Classification Description: Level 1 – Confidential

⚠ This is Protected Data

Information will be classified as **Confidential** if it meets at least one of the criteria below:

1. Exposure Poses a Severe Risk

Confidential data includes information whose unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result in severe damage to the University, its students, employees, or business partners. Financial loss, damage to the University's reputation, and legal action could occur if such information is not properly safeguarded.

2. Legal Obligation

Information for which disclosure to persons outside of the institution is strictly governed by State or Federal statute with the intention to protect the privacy of an individual's information.

3. Other Sensitive Information

Information deemed by the University as highly sensitive, typically reserved solely for use within the college and limited to those employees with a specific need to know.

Examples of Level 1 Confidential information include but are not limited to:

- Passwords or credentials that grant access to Confidential and Private data
- Personal Identification Numbers (PINs)
- Birth date combined with last four digits of SSN and name
- Credit card numbers with cardholder name
- Tax ID with name
- Driver's license number, state identification card, or other forms of national or international identification (such as passports, visas, etc.) in combination with name
- Social Security number and name
- Health insurance information
- Medical records related to an individual
- Psychological counseling records related to an individual
- Bank account or debit card information in combination with any required security code, access code, or password that would permit access to an individual's financial account
- Electronic or digitized signatures
- Personnel records
- Criminal background check results

Classification Description: Level 2 – Private

This is Protected Data

Information may be classified as **Private** if it meets at least one of the criteria below:

1. **Sensitive Nature of Data**

Information which must be protected due to proprietary, ethical, contractual or privacy considerations.

2. **Exposure Poses a Moderate Risk**

Information which may not be specifically protected by statute, regulations, or other legal obligations or mandates but for which unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could cause financial loss, damage to the University's reputation, violate an individual's privacy rights, or subject the University to legal action.

Examples of Level 2 Private information include but are not limited to:

Identity Validation Keys (name with)

- Birth date (full: mm-dd-yy)
- Birth date (partial: mm-dd only)

Employee Information

- Employee net salary
- Home address
- Personal telephone numbers
- Personal email address
- Payment history
- Employee evaluations
- Pre-employment background investigations
- Mother's maiden name
- Race and ethnicity
- Sexual orientation
- Parents' and other family members' names
- Birthplace (City, State, Country)
- Gender
- Marital status
- Physical description

Student Information — Educational Records not defined as "directory" information as defined in FERPA and, typically:

- Grades
- Courses taken
- Schedule
- Test Scores
- Advising records
- Educational services received
- Disciplinary actions
- Student photo

Various Identifiers — Educational Records not defined as "directory" information as defined in FERPA, typically:

- Photo (taken for identification purposes)
- Library circulation information
- Trade secrets or intellectual property such as research activities
- Location of critical or protected assets
- University attorney-client communications

Classification Description: Level 3 – General

Information which may be designated by Stockton University or by State or Federal statute as generally available and/or intended to be provided to the general public.

Disclosure of this information does not expose the University to financial loss or jeopardize the security of the University's information assets.

Information at this level requires no specific protective measures but may be subject to appropriate review or disclosure procedures at the discretion of Stockton University in order to mitigate potential risks.

Additional Definitions

Basic Elements of a Student's Record

1. Demographic data which includes: legal name, social security number, date of birth, sex, citizenship, veteran's status, home and mailing addresses, emergency contact address, and parent or guardian's name, Z-Number.
2. Transcript Data which encompasses all courses attempted and grades received, total transfer credits accepted, all credit by examination units, date of graduation, degree earned.
3. Related Items. Academic materials which the student may have requested in writing be placed in his/her file.
4. Letters of Recommendation. Letters of recommendation will be placed in a student's file only if the student expresses in writing an authorization to do so. Letters are purged after graduation or inactivity.
5. Violations of Campus Conduct Code. This would include the regulations(s) violated, time and place of violation, and sanctions applied.

Information sourced from: [University Policy II-91](#)

c. Data Storage and Retention

i Electronic Document Backup and Archive Schedule

	BACKUP FREQUENCY	BACKUP RETENTION PERIOD
Banner Database	Continuous	Indefinite
	Daily	
	Quarterly	
Faculty and Staff Computer <i>My Documents</i> Folders and Files	Continuous	Unlimited
	Daily	
Faculty and Staff (Select Users)	Daily	3 years
www.stockton.edu Web Pages	Daily	Unlimited
Blackboard Course Content	Maintained by service provider	
Virtual Infrastructure	Daily	4 weeks

i Data Retention Schedule

GOOGLE	RETENTION PERIOD
Email (Gmail)	Indefinite
Files (Drive)	Indefinite
MICROSOFT (Office 365)	RETENTION PERIOD
Email (Outlook/Exchange)	Indefinite
Files (OneDrive)	30 days after deletion

i This policy defines what kind of backups are performed, how often data should be backed up, what software/hardware or cloud service is used for backups, where backups are located, and authorized personnel. It also includes the procedures associated with the retrieval of files, folders, or email from archive media.

Data Backup

University electronic documents and records (data) that are stored on systems managed by Information Technology Services are routinely backed up.

Backups are made to safeguard data against storage equipment failure or accidental data loss and to provide reliable recovery of data. Safeguarded data are backed up to devices other than the source device. Some systems are backed up in real-time, effectively creating a duplicate version of data. The critical data that are duplicated in real-time are also copied daily to another storage device as an added precaution. Backups of critical data that may be needed for disaster recovery purposes are taken to an off-site storage facility. These backups are retained for a limited period of time, usually several weeks.

In addition to safeguarding data against equipment failure or accidental loss, it is important to preserve certain institutional data for possible future reference and use. Data archives are preserved snapshots of data at a point in time. It should be noted that restoring archived data can be an involved and time consuming process. Information system upgrades occur periodically. These upgrades do not always recognize earlier versions of the same system. Accordingly, the restoration of data may involve rebuilding an earlier version of a system or writing a program to extract the needed data.

Restrictions

Users of Stockton computing resources, in regards to portable storage media, must refrain from:

- using the device to store confidential information
- inserting portable storage into Stockton systems from an unknown origin
- using removable media to insert malware into Stockton systems

Securing Institutional Data on Backup or Removable Storage Devices

Any personally identifiable or otherwise confidential data that is stored on personal computers, cloud servers, removable storage devices, or transmitted via email or otherwise electronically transferred must be stored and transferred in a secure manner.

Information sourced from: [University Procedure 4200](#)

i The following page denotes the application of Windows BitLocker into the information system. Specifically noting how the information system utilizes BitLocker as an at rest data-protection solution to protect against unauthorized access. BitLocker provides encryption for full drives and portable drives.

Windows BitLocker

BitLocker Drive Encryption is a data protection feature that integrates with the operating system and addresses the threats of data theft or exposure from lost, stolen, or inappropriately decommissioned computers.

BitLocker provides the most protection when used with a Trusted Platform Module (TPM) version 1.2 or later. The TPM is a hardware component installed in many newer computers by the computer manufacturers. It works with BitLocker to help protect user data and to ensure that a computer has not been tampered with while the system was offline.

On computers that do not have a TPM version 1.2 or later, you can still use BitLocker to encrypt the Windows operating system drive. However, this implementation will require the user to insert a USB startup key to start the computer or resume from hibernation. Starting with Windows 8, you can use an operating system volume password to protect the operating system volume on a computer without TPM. Both options do not provide the pre-startup system integrity verification offered by BitLocker with a TPM.

In addition to the TPM, BitLocker offers the option to lock the normal startup process until the user supplies a personal identification number (PIN) or inserts a removable device, such as a USB flash drive, that contains a startup key. These additional security measures provide multifactor authentication and assurance that the computer will not start or resume from hibernation until the correct PIN or startup key is presented.

Information sourced from: <https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview>

Data Protection

i The following table lists specific data-protection concerns and how they are addressed in Windows 10.

- Modern Windows devices are increasingly protected with BitLocker Device Encryption out of the box and support SSO to seamlessly protect the BitLocker encryption keys from cold boot attacks.
- Network Unlock allows PCs to start automatically when connected to the internal network.
- BitLocker pre-provisioning, encrypting hard drives, and Used Space Only encryption allow administrators to enable BitLocker quickly on new computers.
- BitLocker supports offloading encryption to encrypted hard drives.
- BitLocker supports encrypted hard drives with onboard encryption hardware built in, which allows administrators to use the familiar BitLocker administrative tools to manage them.
- Used Space Only encryption in BitLocker To Go allows users to encrypt removable data drives in seconds.
- BitLocker requires the user to enter a recovery key only when disk corruption occurs or when he or she loses the PIN or password.
- Modern Windows devices are increasingly protected with BitLocker Device Encryption out of the box and support SSO to help protect the BitLocker encryption keys from cold boot attacks.

Information sourced from: <https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-device-encryption-overview-windows-10>

d. Data Transmission

Secure Transmittal of Data

Any personally identifiable or otherwise confidential data that is stored on personal computers, cloud servers, removable storage devices, or transmitted via email or otherwise electronically transferred must be stored and transferred in a secure manner. Institutional data may only be transmitted to or from an external site, including external email accounts for specific job related purposes. Institutional data that are electronically transmitted to or from an external site, including an external email account, should be securely transmitted. When transmitted via email, sensitive data should be encrypted, password protected and sent as an attachment to the email message. The password for the encrypted attachment must always be transmitted under separate cover or via telephone or voicemail. Some employees may for specific job related purposes need to transmit institutional data to a third party (e.g., Financial Loan Processor, Bank, Credit Union, transfer institution). Whenever institutional data is transmitted to a third party, it must be transmitted via a secure communication protocol, such as TLS or Secure FTP. Contact Information Technology Services if you have questions concerning the secure transmittal of data.

 Stockton University implements a multi-faceted approach to encrypting mobile devices.

Encrypting Institutional Data

- Institutional data that is stored on a privately owned computer, mobile or removable storage devices, or cloudbased facility should be encrypted. Contact Information Technology Services for advice or assistance, if needed.
- Mobile computers, flash drives or removable drives acquired by the university for administrative purposes must be equipped and configured to automatically encrypt data.
- The use of encryption, the labeling of a communication as private, the deletion of a communication or any other such process or action, shall not diminish the University's rights in any manner.

Information sourced from: [University Procedure 4200](#)

Data Flow Control

Alerting on Questionable Activity

- Email forwarding rules
- Escalation of privileges
- High volume of outbound email
- Questionable content (SSN, Bank Account Numbers, etc)

Block Outbound Messages

- Prevent users from sending US Social Security Number outside of the Stockton.edu domain

AppLocker Domain Policy

- Prevent ransomware and other malware from infecting domain systems

e. Data Destruction

Risk Management - Records Retention and Disposal

i The Office of Risk Management is responsible for following the requirements of the NJ Division of Revenue and Enterprise Services, Records Management Services for all records retention and disposition schedules; research and development policies on electronic records; aid in the inventory and appraisal of records for reorganization or disposition projects; and approval routine records disposal requests.

Information sourced from: <https://stockton.edu/risk-management/records.html>

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 lock their workstation when they are away from their work area.

1. 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.
2. 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.
3. When computers are relocated for use within the University, confidential data is removed. The University periodically contracts for the destruction and removal of decommissioned servers, hard disk drives, and other technology containing sensitive information.
4. Windows-based University issued laptops are configured to automatically encrypt data stored on the hard disk drive.

3. Safeguarding Information Systems

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

System/Application Management

Information Systems Control

Nonpublic information (i.e., data that is deemed confidential or private) obtained through University administrative software systems must be treated as sensitive, and can only be used in connection with a person's job responsibilities, and for official use only.

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.

To better address the elements and objectives of the Gramm-Leach-Bliley Act (GLBA) and FTC Regulation 16 CRT Part 314, internal plans /practices have been developed.

Administrative Applications Security

Banner, which is used to support the University's administrative operations, provides for user account, online form, data element and data value security that is capable of restricting persons from updating or viewing of database elements selectively.

The Division of Information Technology Services administers security for the University's administrative computing systems, excluding system level security associated with financial records and human resource systems, which are administered by the Office of Budget and the Office of Human Resources, respectively.

The Division of Information Technology 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 Division of Information Technology Services staff responsible for maintaining application software systems are granted online application access accounts to production, test, and training systems. Programmers and other authorized Division of Information Technology Services staff may be granted limited access to production system data that are used to configure and control system processes. Division of Information Technology Services staff that are granted access to data must carefully observe security standards and practices.

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 online 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 Information Technology Services staff. Changes to source code, including patches supplied by the vendor, must be 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 Information Technology Services staff.

Integrity Assurance Controls

The following are examples of controls, which must be followed, to ensure application system integrity:

1. Changes to Banner must be made first made on the test system prior to their transfer to production.
2. Users must develop testing data and acceptance plans.

Account Management

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 Usage of Computing and Communication 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 Usage of Computing and Communication Facilities, only persons authorized by the Chief Information Officer may be granted computing accounts. Access to and use of administrative computing facilities may be granted to appropriate personnel by the Chief Information Officer or by the recognized custodian of the data for which access is requested.

Computer accounts or other identifiers used to gain access to computing and communication technology or data may be used only by the individual authorized to use the account or identifier, and only for the purposes for which the account was authorized. Users shall not capture, decipher or record other users' account information, passwords, PINs, or keystrokes, nor use or attempt to use another individual's account or personal information.

Account Practices:

1. The use of group or shared accounts should be avoided.
2. Passwords for administrative computer accounts are automatically expired every 180 days.
3. Passwords for Oracle accounts are automatically expired every 90 days.
4. Computer accounts that permit access to administrative or other protected data are reviewed and access de-provisioned whenever account holders resign their position, retire, or otherwise leave the University.

Identifies and selects the following types of information system accounts to support organizational missions/business functions:

- Assigns account managers for information system accounts to accomplish life cycle activities;
 - Manage through a life cycle consisting of establishing, activating and modifying accounts; periodically reviewing accounts; and disabling, removing or terminating information system accounts, defined as individual, group, system and role-based accounts defined as administrator, application, guest and temporary.
- Establishes conditions for group and role membership;
- Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;
 - Document within applicable system security plans a description of authorized system users, criteria group and role accounts' membership with access privileges, and other applicable account attributes.
- Requires approvals by the office of Information Security for requests to create information system accounts;
- Creates, enables, modifies, disables, and removes information system accounts in accordance with university policies and procedures;
- Monitors the use of information system accounts;
 - Managers and supervisors shall oversee and review users' activities to enforce use of information system access controls.

Notifies account managers:

- When accounts are no longer required;
- When users are terminated or transferred;
- When individual information system usage or need-to-know changes;

Authorized access to the information system is based on:

- User account request documentation is completed in full prior to account creation,
 - At a minimum, the request provides the user's name, clearance level, and all rules of behavior have been read and acknowledged in writing, and explicitly details the access privileges requested.
- A valid access authorization;
- Intended system usage;
- Other attributes as required by the organization or associated missions/business functions;
- Reviews accounts for compliance with account management requirements [annually];
- Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.

Account Security: Preventing Against Improper Use

To protect Stockton University computing and communication technology against unauthorized or improper use, and to protect authorized users from the effects of unauthorized or improper usage, the CIO or appropriate University supervisory authority has the right, with or without notice, to monitor, record, limit or restrict any user account, access and/or usage of account.

If the Chief Information Officer (CIO) or appropriate University supervisory authority believe that an alleged violation of these Standards or other regulations presents a risk to the integrity and/or the orderly conduct of the operation of the University's computing and communication technology, the user may be subject to restricted access or loss of access to such technology; disciplinary action under applicable University policies and procedures up to and including termination and/or expulsion from Stockton University; and where appropriate, civil and/or criminal liability.

Users without the authorization of the CIO or CIO's designee shall not attempt or knowingly seek, provide, view, use, delete, or modify information in, or obtain copies of files or programs belonging to other computer or telephony users without the permission of those users. Searching through non-public directories, libraries, or any other storage media for unauthorized information is prohibited. Further, computer users shall not use the computing and communication technology to plagiarize or claim the intellectual or literary property of others.

Information sourced from: [University Procedure 4200](#)

Separation of Responsibility

The organization:

- Separates individuals by recommended duties of individuals, based on roles and responsibilities, to be approved and accepted by the office of Information Security;
- Documents separation of duties of individuals;
- Defines information system access authorizations to support separation of duties.

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

1. All official documents, such as transcripts or diplomas, must be stored, controlled and accounted for by the designated system custodian.
2. All official documents must feature appropriate confidentiality warnings/statements.
3. All runs involving negotiable paper must take place in a physically secured location during weekday shifts with at least two people present.
4. Division of Information Technology Services personnel must not run update processes or change data on production systems unless specifically directed to do so by the appropriate data custodian. Changes are coordinated between data custodians, information security, and banner application programming team.
5. All production jobs must be requested by user offices and approved by data custodians.
6. Changes to application systems may not occur without written user request and approval of data custodian.
7. No user may authorize their own access (serve as the signatory on an access request form), with the exception of the Chief Information Officer or University President.

Data Management

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, online 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 online 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:

1. Verify the reliability and integrity of data using sound, well-defined verification methods.
2. Additionally, processes that update data in mass should be tested in non-production environments.
3. Provide thorough documentation regarding the practices that employees must follow while processing and verifying data.

Data Security

Appropriate safeguards must be taken to ensure 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 private data must be stored in a physically secured area or encrypted using a strong password or key. The Division of Information Technology Services is responsible for safeguarding institutional data that resides on the University's central computing facilities. Systems containing confidential or private information must require users to authenticate themselves using industry accepted account and password authentication methods. Access to systems and/or data is granted by the relevant data owner, and by proxy, any delegated data custodian. Security controls are evaluated and user access reviews are conducted by the Information Security team at the request of relevant data owners/custodians, and periodically as part of ongoing operational security initiatives.

System administrators, operators and certain authorized staff may be allowed full access to files and programs during development, maintenance, backup/restore operations, or in acting to fulfill assigned University duties or in safeguarding the integrity and reliability of computing and communication technology. Staff members who are authorized such access shall respect the confidentiality of data stored. In the event that unauthorized computer or telephony system use is suspected, the staff member who detects, or is informed of the suspected violation, must notify the Chief Information Officer or appropriate University supervisory authority, as well as the Stockton Police Department.

E-mail system files and messages can be stored locally or offsite by Information Technology Services and may be backed up by Information Technology Services in alternate methods as a precaution against accidental loss or hardware failure. As such, systems and backups may contain privileged, sensitive, confidential, and/or personally identifiable information. The duplication and/or exfiltration of institutional data containing any of the aforementioned properties is strictly prohibited and may result in the violation of State or Federal law.

Information sourced from: [University Procedure 4200](#)

Asset Management

i Information Technology Services (ITS) maintains a variety of information systems that assist in asset identification, monitoring, and configuration of institutional assets.

In addition to technical controls, directive controls also govern the use and issuance of technology. Scenarios for new issuance, termination, and loaner technology are outlined below.

Internal Procedures

New Issuance

- ITS approves equipment purchases
- ITS help desk creates a ticket for initial setup of the equipment
- ITS help desk enters the information into asset management systems
- ITS help desk interfaces with equipment recipient for configuration and training

Terminations

- ITS help desk is notified of an employee's last working day
- ITS help desk performs a discovery for potentially affected assets/equipment
- ITS help desk collects the assets for evaluation and re-issuance or decommissioning

Equipment Loans

- Mobile Devices with commercial wireless network service may be issued to employees who meet specific job-based eligibility criteria and have approval of their divisional cabinet member.
- Information Technology Services maintains a limited equipment inventory of technology that may be circulated
- Faculty, staff and students are responsible for borrowed equipment while it is in their possession
- Loan of equipment is for the duration of the circulation period unless special arrangements are made at the time of the request.
- At the end of the circulation period, the request may be renewed.
- Renewal is at the discretion of Information Technology Services and will be determined by general demand for the equipment and use.
- ITS help desk creates a ticket to document each individual case
- Follow-ups are periodically performed
- Faculty, students and staff may borrow designated technology equipment for use off campus at the discretion of Information Technology Services personnel.
- All equipment is otherwise limited to use at campus locations only.

Information sourced from: [University Procedure 4148](#)

Technical Controls

Ticketing System

- The help desk ticketing and inventory management system is used to document support issues, and maintains device information

Remote Support

- ITS utilizes a cloud-based, multi-factor authenticated remote support tool to provide support to members of the University community

Additional Technical Controls

- ITS utilizes additional technical controls to monitor, detect and respond to support requests and information security threats
- These controls may include data loss prevention mechanisms, network access control, device management policies, and system-level alerting

Network Management

Network and System Security

Network systems must be designed to reasonably limit the risk of unauthorized access to administrative information systems.

The information system is configured to enforce approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with university policy, procedures and standards. Additionally, appropriate safeguards must be in place to monitor network security and respond to potential attempts to breach security. 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 virtual desktop infrastructure (VDI) or a virtual private network (VPN) when accessing systems via the Internet. Faculty or staff requiring access to systems via VPN or elevated VDI must request access through the Division of Information Technology Services. Access cannot be provided where in the judgment of the Chief Information Officer such access may compromise system security. The transmission of confidential or private data over the internet to web-based applications or servers must utilize trusted communications protocols, such as TLS.

Reliability and Integrity of Facilities

Users of computing and communication technology shall not knowingly develop, use, or transmit through the University's technology system any programs, data, or technology that interferes with, infiltrates, or damages computing and communication technology, or violates any civil or criminal law.

Users of the University's computer and communication technology shall exercise great care to prevent or protect the use of programs or utilities accessed through such technology and shall not engage in actions that interfere with, infiltrate, or damage such technology.

Users shall not engage in any activity that may lead to unauthorized access to systems, accounts, or data on the University's computing and communication technology. Additionally, users shall not attempt to circumvent or subvert system or network security measures. Further, implementing methods that mask network traffic for unauthorized or unlawful purposes is prohibited. Any defects discovered in system security must be reported immediately to the Chief Information Officer.

Information sourced from: [University Procedure 4200](#)

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 Information Technology 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 Chief Information Officer or the University President.

PCI Compliance

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 transmitted over non-secured channels. Cardholder data stored in hard copy 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.

According to PCI standards: "At a minimum, cardholder data contains the full Primary Account Number (PAN), 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."

4. Responding to Information System Security Threats

i The following are measures that should be taken to protect against security threats.

Incident Response

i The University maintains practices and plans associated with Incident Response.

The following is an overview of those practices and plans:

- Incident Handling
- Incident Monitoring
- Incident Response
 - Training
 - Testing
 - Assistance
- Incident Reporting

Information Security Threats

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

Examine Security Logs

The Division of Information Technology Services collects, aggregates, and stores logs related to authentication and configuration management. These logs are periodically reviewed by system administrators and used by incident handlers for investigations.

Evaluate Suspected Security Breaches

Suspected security breaches must be reported to the University's Chief Information Officer (CIO). The information security team conducts investigations based on reported and detected incidents. The Chief Information Officer leads the evaluation of suspected security breaches that may have disclosed protected information. As necessary, the CIO will relay information to University's General Counsel, Risk Management, and University Senior Leadership.

Notify Affected Persons

In cases where the University 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 affected person.

Information sourced from: [University Procedure 6902](#)

Procedure for Using University Communication Systems/Tools to Disseminate Messages to the Stockton Community

Mass email is any email message sent to the entire campus or a large subset of the same (e.g., all students, all undergraduates, all graduate students, all faculty, all staff).

Mass email is appropriate for information that pertains to the majority of the recipients and meets at least one of the following criteria:

- Provides information essential to the operation or execution of University business;
- Provides information employees need to perform their jobs or engage with the University;
- Provides obligatory information employees need to know as state employees or state officials;
- Alerts the campus community to situations about health or safety risks as defined in emergency notification procedures;
- Announces major campus events (e.g., Convocation, Commencement, Faculty Assemblies, noteworthy athletic events);
- Alerts the campus community of key processes, procedures, services, and deadlines from Human Resources, Facilities and Operations, and Information Technology Services;
- Communicates important information from the President, Provost, or other University senior leadership

Information sourced from: [University Procedure 4155](#)

Conduct Periodic Security Review

On an annual basis, the University's network and administrative systems are tested to determine whether they are meeting industry standards for access control and security.

Definition

A computer security incident is an adverse activity occurring on the university's computer network or a host computer that breaches the security of or significantly blocks access to computer systems or applications. A potential but not yet occurring activity that threatens the security or legitimate access to the university's computer systems or applications is referred to as a computer security threat. The following describes the university's procedure for monitoring, identifying, assessing and responding to security threats and incidents.

 The Chief Information Officer is responsible for involving and informing campus departments and external parties, assembling and overseeing the response team, and directing the plan of action during a computer security incident. Members of the IT management team have responsibility for assessing potential or actual impact of the threat or incident, developing containment procedures, executing approved plans of action for containment and restoration, collecting evidence for forensic investigation and post-mortem reporting. Under circumstances where immediate action is necessary, IT management may execute a plan of action without prior approval. In the case of a critical security incident, the Chief Information Officer is required to present to the University President a summary report describing the cause, consequence, response, containment, and restorative action plan.

i The following page is an overview of the Incident Response process the information system incorporates.

Definition

A computer security incident is an adverse activity occurring on the university's computer network or a host computer that breaches the security of or significantly blocks access to computer systems or applications. A potential but not yet occurring activity that threatens the security or legitimate access to the university's computer systems or applications is referred to as a computer security threat. The following describes the university's procedure for monitoring, identifying, assessing and responding to security threats and incidents.

Incident Response Phase Overview



For more information: [Incident Response Standards](#)

Assignment of Severity

An identified network security threat is immediately assigned a level of severity as outlined below:

High Severity

A known and present or imminently present security threat with a high probability of 1) systemically compromising security access controls that protect audit significant, sensitive or confidential information assets, or 2) causing wide-scale, sustained, denial of access to mission-critical or audit significant information resources. Security events categorized as "High Severity" are acted upon immediately with the goal of resolving and remediating the incident within 1 business day.

Medium Severity

A known security threat with medium probability of occurring on campus and 1) systemically compromising security access controls that protect audit significant, sensitive or confidential information assets, or 2) causing wide-scale, sustained, denial of access to mission-critical or audit significant information resources. Security events categorized as "Medium Severity" are acted upon within 1 business day with the goal of resolving and remediating the incident within 2 business days.

Low Severity

A known security threat with low probability of occurring on campus and 1) systemically compromising security access controls that protect audit significant, sensitive or confidential information assets, or 2) causing wide-scale, sustained, denial of access to mission-critical or audit significant information resources. Security events categorized as "Low Severity" are acted upon within 1 week with the goal of resolving and remediating the incident within 1 week.

i The Chief Information Officer is responsible for involving and informing campus departments and external parties, assembling and overseeing the response team, and directing the plan of action during a computer security incident. The Security Administrator and Director of Telecommunications and Network Services have responsibility for assessing potential or actual impact of the threat or incident, developing containment practices, executing approved plans of action for containment and restoration, collecting evidence for forensic investigation and post mortem reporting. Under circumstances where immediate action is necessary, the Security Administrator or Director of Telecommunication and Network Services may execute a plan of action without prior approval.

In the case of a critical security incident, the Chief Information Officer is required to present to the University President a summary report describing the cause, consequence, response, containment and restoration action plan, and recommendations for prevention.

Incident Escalation Processes

i Emails to information.security@stockton.edu and calls to the Information Security Unit.

w Inquiries are responded to by members of the Information Security Team.

i Emails to helpdesk@stockton.edu and calls to 609-652-4309.

w Inquiries are responded to by members of the Help Desk. Relevant matters are escalated to the Information Security Team.

i Emails to phishing@stockton.edu.

w Inquiries are responded to by members of the Communications and Infrastructure Team. Relevant matters are escalated to the Information Security Team.

Vulnerability/Patch Management

Vulnerability Management

i Stockton University performs the following vulnerability scanning:

- Quarterly external vulnerability scans
- Monthly internal vulnerability scans

Patch Management

i Information Technology Services maintain a variety of practices and standards related to patch management.

- Infrastructure Patch Management
- Database Patch Management
- Operating System Image Patch Management
- Workstation Application Patch Management

5. Appendix

Appendix A. Listing of Relevant University Policies and Procedures

University Policies		
Number	Title	Link
II-81	Computing and Communication Technology Access and Use	https://stockton.edu/policy-procedure/documents/policies/II-81.pdf
II-85	Use of University Communication Systems/Tools	https://stockton.edu/policy-procedure/documents/policies/II-85.pdf
VI-89	Internal Audit Policies	https://stockton.edu/policy-procedure/documents/policies/VI-89.pdf
VI-91	Identity Theft Prevention Program	https://stockton.edu/policy-procedure/documents/policies/VI-91.pdf
VI-92	Files and Records - Review, Retention, and Retirement	https://stockton.edu/policy-procedure/documents/policies/VI-92.pdf
University Procedures		
Number	Title	Link
4146	Technology Equipment Circulation	https://www.stockton.edu/policy-procedure/documents/procedures/4146.pdf?1610034677445
4148	Events Requiring Audio, Video, Information Technology Support and/or Production	https://stockton.edu/policy-procedure/documents/procedures/4148.pdf
4152	Technology Equipment Losses	https://www.stockton.edu/policy-procedure/documents/procedures/4152.pdf?1610034677445
4155	Procedure for Using University Communication Systems /Tools to Disseminate Messages to the Stockton Community	https://www.stockton.edu/policy-procedure/documents/procedures/4155.pdf?1610034677445
4200	Acceptable Usage Standards	https://stockton.edu/policy-procedure/documents/procedures/4200.pdf
6420	Mobile Devices and Commercial Wireless Network Service	https://stockton.edu/policy-procedure/documents/procedures/6420.pdf
6421	Internal Audit Procedures and Standards	https://stockton.edu/policy-procedure/documents/procedures/6421.pdf
6902	Identity Theft Prevention Program	https://stockton.edu/policy-procedure/documents/procedures/6902.pdf
6912	Information Security Compliance (GLBA/FERPA)	https://stockton.edu/policy-procedure/documents/procedures/6912.pdf