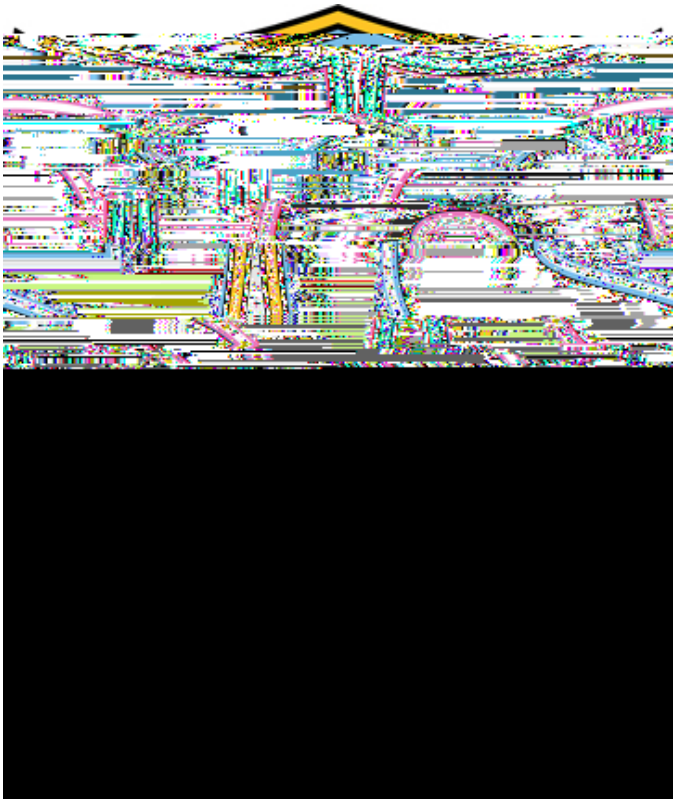
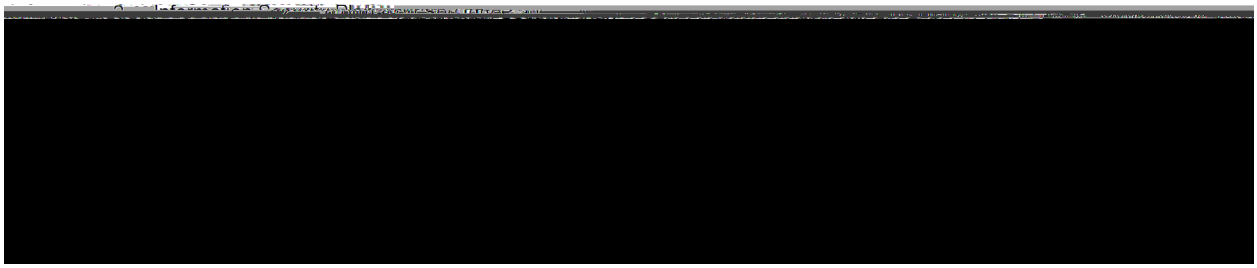
STOCKTON UNIVERSITY

INFORMATION SECURITY PLAN





Updated June, 2021

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

Information Systems
Information systems consist of the software, 62.l 54 452.l 54 454a3 f 0.866systl 54 454a3 f. 0.866systl Systems

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

The purpose of this section is to highlight the different aspects of data management that have been established by the University to

-
-
-
-
-

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.

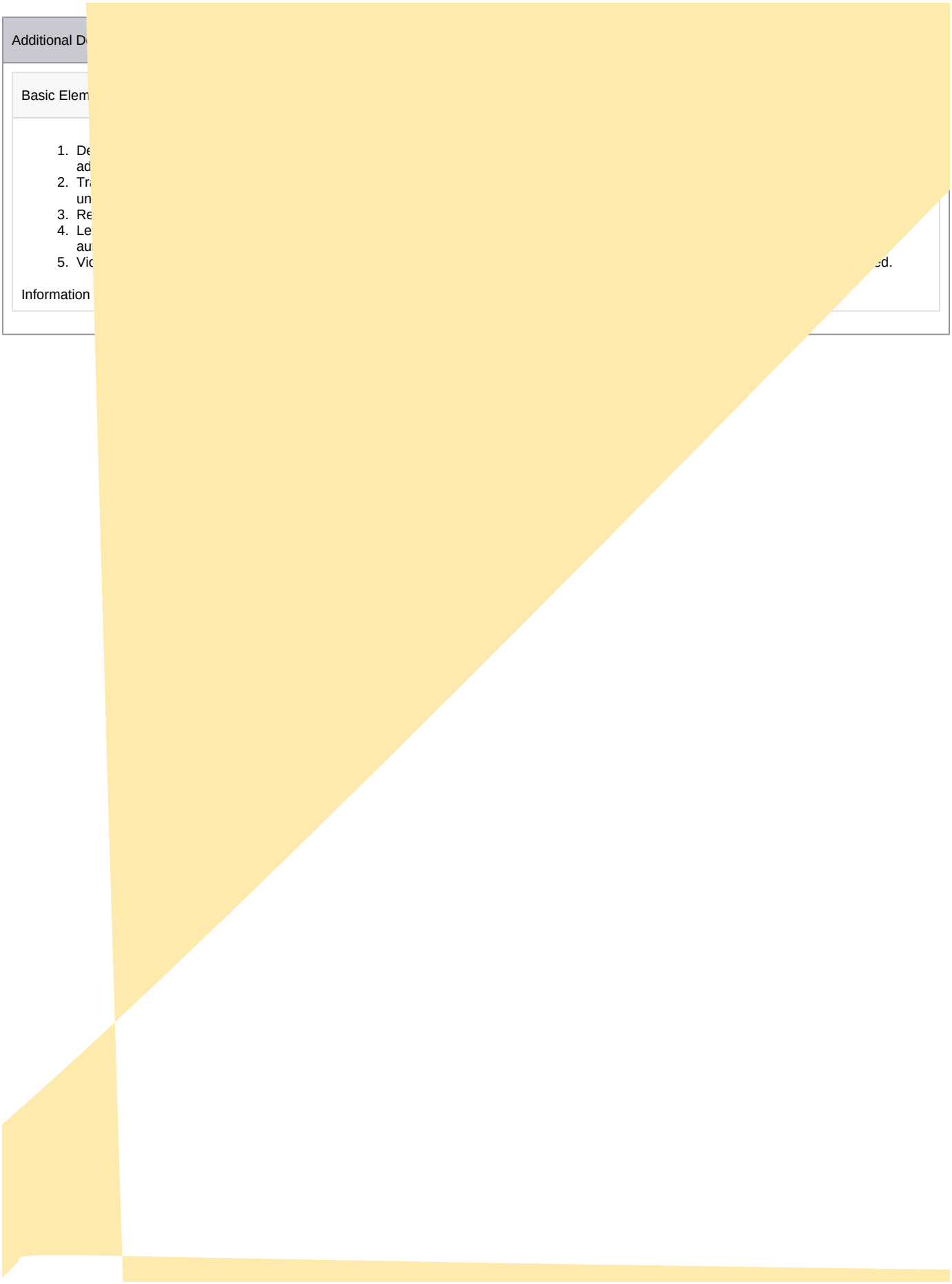
Personally Identifiable Information
Personally Identifiable Information (PII) refers to any data that identifies or can be used to identify, contact, or locate the person to whom such

Guidelines for Safeguarding Personally Identifiable and Confidential Information

b. Data Classification

Data Classification
Information may be classified when needed into one of the following Level 1 - Confidential Level 2 - Private Level 3 - General The three levels described below are meant to be illustrative, a

Classification Description: Level 1 – Confidential
This is Protected Data Information will be classified as Confidential if it mee 1. Exposure Poses a Severe Risk Confidential data includes information wh severe damage to the University, its stu legal action could occur if such informa 2. Legal Obligation Information for which disclosure to p the privacy of an individual's inform 3. Other Sensitive Information Information deemed by the Univ with a specific need to know. Examples of Level 1 Confidential infor • Passwords or credentials t • Personal Identification Nu • Birth date combined with • Credit card numbers wi • Tax ID with name • Driver's license numb combination with na • Social Security nur • Health insurance • Medical records • Psychological c • Bank account ode, or password that would permit access to an individual' • Electronic o • Personnel • Criminal h


Additional D
Basic Elem
1. De
ad
2. Tr
un
3. Re
4. Le
au
5. Vi
ed.
Information

-
-
-

-

-

-

e. Data Destruction

Risk Management - Records Retention and Disposal

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.
2.
3.
4.

3. Safeguarding Information Systems

1.
2.

Account Management

Account Security

Faculty and staff may have access to administrative computing accounts, as needed, in accordance with their job responsibilities.

1.
2.
3.
4.

-
  -
-
-
  -
-
-
-
  -
-
-
-
  -
-
-
-
-

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

-
-
-

1.
2.
3.
4.

5.
6.
7.

Asset Management

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

-
-
-
-

4. Responding to Information System Security Threats

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

Incident Response

The University maintains practices and pla

The following is an overvi

Conduct Periodic Security Review

Incident Escalation Processes

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

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

Emails to phishing@stockton.edu .

-
-

-
-
-
-

5. Appendix
