Guidelines for Safeguarding Personally Identifiable and Confidential Information from Unauthorized or Accidental Disclosure

Introduction

The purpose of this Statement is to reaffirm the Standards that apply in the matter concerning the safeguarding of administrative, personally identifiable or confidential data that has been entrusted to the University or to persons working on behalf of the University. These guidelines are applicable to the University's computing and communications facilities, or any facility, service or device (privately owned, leased or granted), where such entrusted data are stored or accessed.

Terms and Definitions

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 (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 and credit card information. 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 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.

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

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 mission-centered programs of the institution. Authorization for the use of and/or access to the University's computing and

communication facilities is granted by the Executive Director of Computer and Telecommunication Services and the Director or supervisor of the organizational unit that is the recognized steward and custodian of the data for which access is requested. 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.

SYSTEM	CUSTODIAN (Director or head of)
Student Information System	
Admissions	Admissions Office
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
Human Resource System	
Payroll	Payroll Office
Labor Distribution	Office of the Dir. of Budget
Personnel Records	Human Resources Office
Benefit Record	Human Resources Office
Alumni and Development System	
Advancement Records	Alumni and Development
Alumni Records	Alumni and Development
Finance System	
Financial Account	Office of the Dir. of Budget
Accounts Payable	Office of Accounts Payable
Purchasing	Purchasing Office
E – Mail Systems	Office of Computer Services
Library Management System	Office of the Director of the Library
CBORD Board and Debit System	Bursar's Office
Central Stores	Central Stores
Fixed Asset Inventory	Office of the Controller
Academic facilities and systems	Office of Computer Services
Housing Management systems	Office of Housing and Residential Life
Facilities Maintenance systems	Office of Plant Management
Learning Management systems	Office of E-Learning

Anyone who has access to institutional data must act to properly safeguard such data against unauthorized or accidental disclosure to a third party.

Following are specific guidelines for the proper protection of institutional data. If you have any questions concerning data security, please contact the Office of Computer and Telecommunication Services.

Secure Access and Storage of Institutional Data – Institutional data must be protected from unauthorized access or accidental disclosure. Access to institutional data must, to the extent possible, be restricted using strong passwords (e.g., a password of greater than 8 characters, including special characters and numbers).

Securing Institutional Data on Backup or Removable Storage Devices– Employees may for specific job related purposes and with the approval of the appropriate data custodian copy or create and store institutional data to a removable storage device, PC, mobile device, cloud-based or remote facility. Removable media and mobile devices containing institutional data should always be kept in a place that is safe from theft, unauthorized access or accidental disclosure. Employees or other authorized personnel must take care to promptly remove institutional data that has been placed on desktop or portable computers, removable media, or cloud-based or remote facilities when the data is no longer needed for the specific purpose.

Device Access Security – Desktop and mobile devices that contain or provide access to institutional data must be password protected against unauthorized access. These computers and devices should be shut down when not in use for extended timeframes. Additionally, they should, when possible, be configured to require password re-authentication after no more than 20 minutes of inactivity.

Encrypting Institutional Data – Institutional data that is stored on a privately owned computer, mobile or removable storage devices, or cloud-based facility should be encrypted. Cost-free methods for encrypting and protecting data are readily available for most devices. (See detailed instructions at http://intraweb.stockton.edu/eyos/computer_services/Instructions/Compressing%20Files%20in%20Windows%207%20and%20XP.pdf.) Contact the Office of Computer 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.

Secure Transmittal of Data – 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, institutional 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 3rd party (e.g., Financial Loan Processor, Bank, Credit Union, transfer institution). Whenever institutional data is

transmitted to a 3rd party, it must be transmitted over a secure communication protocol, such as SSL, or Secure FTP. Contact the Office of Computer Services if you have questions concerning the secure transmittal of data.

Securing Paper Files – Institutional data that is kept in hard copy form must also be secured and protected. These data should be stored in a location that prevents unauthorized or accidental disclosure.

Effective Measures for Securing Institutional Data on Mobile Devices – Because of their portability mobile devices are more susceptible to loss and theft. Following are specific measures that should be observed to secure institutional data on mobile devices (privately or University owned) that contain institutional data. If you need assistance with any of these measures, please contact the Office of Computer and Telecommunication Services.

- Physically secure your device. Keep it with you or in a secured location.
- Label the device with your name and a phone number where you can be reached in case the device is found and the battery is dead or the device is otherwise unusable.
- Enable device passcode or PIN protection features and select a passcode or PIN that is difficult to guess.
- Enable mobile device idle timeout (e.g., 5 minutes) and locking features.
- If available, enable the feature that will erase data after 10 failed passcode attempts.
- Delete any institutional data from the device when no longer needed
- Encrypt institutional data on the device. All mobile devices and storage (e.g. flash drives) purchased the University must have built in encryption and such encryption must be enabled.
- Record make, model, serial numbers and MAC address of your mobile device and the date and place of purchase. Keep your record in a location separate from your device.
- Enable whole device encryption, if your device is so equipped.
- Enable device tracking features. (e.g., Find My iPhone service)
- Make a secure and encrypted backup of any institutional data (this is needed to not only retrieve data but to also determine the extent of data disclosure, if any, in the case your device is lost or stolen).
- If you are using a cloud service (e.g., iCloud) to back up or otherwise store your data use a strong password.
- Keep software up-to-date to protect against hacking attempts.
- Only load apps or software on your device that come from a trusted source.

Reporting Lost or Stolen Devices or the Suspected Disclosure of Institutional Data – if you know or suspect that University property or a privately owned device containing institutional data has been lost or stolen promptly contact the campus police department. Additionally, promptly notify your unit manager of the incident and the Office of Computer and Telecommunications and request them to attempt to remotely locate your device and wipe email and MS Exchange data (or other data if possible) from the device. Most mobile devices store passwords so that mobile apps can automatically access remote computer applications without having ask the user to supply a username and password. To prevent unauthorized access to your data and accounts you should change your access passwords as soon as possible.