CALIFORNIA STATE UNIVERSITY
SAN BERNARDINO

Safeguarding Confidential Information Standard

CSUSB Information Technology Services

Last Revised: **11/09/2020**

Draft

REVISION CONTROL

Document Title: CSUSB Safeguarding Confidential Information Standard

Author: Dr. Javier Torner

Date	By	Action	Pages
01/22/07	J Torner	Created Standard	All
09/07/11	J Macdonell	Updates to information	All
10/10/13	L Carrizales	Added bullet points to sections 4.2, 4.4, & 4.5	8-11
11/15/13	L Carrizales	Updated information	All
11/25/13	L Carrizales	Document approved by Vice President's Council	All
06/19/15	L Carrizales	Added statement that includes auxiliary units in section 1.0. Added bullet point #2 in section 3.3.	4 and 7
10/12/10	ISET Subcommittee	Updated document and included MFA bullet point	All

Review/Approval History

Date	By	Action	Pages
11/25/13	VP Council	Document approved	All
11/9/2020	IT Governance ISET Subcommittee	Revision Approved	All

1.0 Safeguarding Confidential Information

Introduction:

Recommended practices to ensure the security of confidential information

This document provides recommendations for the implementation of administrative, technical, and physical safeguards designed to:

- Ensure the security of any confidential information in the University's custody in all forms, no matter if that information is contained electronically, written, or in any other format.
- Protect confidential information against any threats or hazards of integrity, unauthorized access, or unauthorized use.

This standard applies to all CSUSB employees, including auxiliary units.

2.0 Definitions

Confidential Information:

Confidential Information means any information not exempted in specific legislation and identified as personal, sensitive, or confidential such as personally-identifiable information, individually-identifiable health information, education records, and non-public information as specified in all applicable federal or state laws, plus CSU and CSUSB policies. Confidential Information includes, but is not limited to, the following examples:

- Social Security number
- Physical description
- Personal address*
- Personal telephone number*
- Ethnicity
- Gender
- Education (except student records which are exempted by FERPA)
- Financial matters
- Performance evaluations
- Verbal or written statements made by or attributed to the individual
- Medical and employment history

Confidential information may include individually-identifiable health information. This includes any information, including demographic information collected from an individual, created or received by a health care provider, health plan, employer, or health care clearinghouse. This includes information that

relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to the individual, or the identification of the individual.

In addition, electronic confidential information is defined as any electronic format which includes an individual's first name or first initial and last name or education in combination with any one or more of the following data elements, when either the individual's name or the data elements are not encrypted:

- Social Security number
- Driver's license number or California Identification Card number
- Account number, e.g., identification number, credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

For the purposes of this standard, confidential information refers to Level 1 and Level 2 information as defined in the CSUSB Data Classification Standard.

*Refer to University Policy and Procedures on Student Records Administration

Unauthorized Disclosure:

Unauthorized Disclosure means to disclose, release, transfer, disseminate, or otherwise communicate all or any part of any record orally, in writing, or by electronic or any other means to an unauthorized person or entity.

3.0 Recommended Practices for Individuals

All confidential information must be cared for with the appropriate level of physical and electronic (logical) security. When working with confidential information users take on the custodial responsibilities for that information. Thus each user who accesses this information has the responsibility to:

- Identify
- Protect
- Communicate
- Maintain

These terms are defined below. Note: These lists are not exhaustive. Each of them are provided to serve as included examples. As technology develops, each of these lists should be expanded to cover additional techniques and devices as appropriate.

Identify:

Identify and inventory where confidential information is stored, processed, or transmitted.

- Confidential information
    - E-mails
    - Electronic documents
    - Printed information (paper)
- Computer information systems
    - Desktop computers
    - Laptops / notebook computers
    - Tablets / Smart Devices
- Local storage device
    - Hard drive
    - PROM (Programmable Read-Only Memory)
    - Internal memory sticks/cards
- Removable media
    - Magnetic (backup) tapes
    - External drives
    - CD or DVD (optical)
    - USB devices
- Remote storage device
    - Shared/mapped drive
    - Network Attached Storage (NAS)
    - Storage Attached Network (SAN)
    - Cloud Storage

Protect:

Protect confidential information against unauthorized access, unauthorized use, loss, or damage.

- Do not share or disclose personal authentication credentials, such as user IDs and passwords or other forms of electronic authentication with other individuals.
- Do not use personal credentials for authentication to provide other individuals with access to any information systems containing confidential information.

- Maintain up to date and install all appropriate security software updates in all computer workstations and laptops and software applications.
- Install and maintain antivirus software in all computer workstations and laptops and set them to auto-update to install the latest antivirus signatures.
- Keep portable equipment and storage devices such as CD, DVD, tapes, USB drives or other removable storage media in an appropriately access-limited location.
- Do not leave computer equipment or portable storage devices unattended.
- Use boot-up (BIOS) passwords for all computer systems and set strong authentication for all user accounts, including any accounts with administrative rights.
- Enable screensaver with authentication (locking passwords) for all computer systems.
- Use caution when accessing email, and do not trust any unexpected emails. Never open an attachment without first verifying its type and checking it with an antivirus program. If in doubt, delete it and/or contact the sender first.
- Position monitors and printers so that others cannot see or obtain confidential or sensitive data.
- When entering or collecting sensitive information from a website make sure that a secure connection has been established. Close your browser and start a new session by starting your browser again before accessing an insecure site. This will prevent others from accessing non-public information which may be stored in the browser's cookies.
- Log out, shut down, or lock the system when leaving your computer unattended at any time.
- Physical safeguards (keys, cipher locks, passwords, etc.) which are used to secure confidential information should be changed occasionally, and should be changed every time someone who formerly had authorized access either leaves university employment, no longer has job requirements which require access, or a key securing such access is lost, stolen or unaccounted for.
- Take particular care at home to keep the system and sensitive data secure from unauthorized access.
- Utilize multi-factor authentication to prevent unauthorized access to information in the event of compromised login credentials.

Communicate:

Communicate your responsibility for confidential information. Choose the information you communicate with care.

- Promptly report any possible unauthorized access, use or loss of information or an information system to the immediate supervisor and the Information Security Office.
- University employees, faculty and staff, including auxiliary employees who have lost/stolen assets, need to follow the procedures outlined by Property Management and submit the appropriate report to the Information Security Office with a copy to their manager.

- Never send confidential information using non-secure applications such as IM, Chat programs, social networks or regular e-mail. Do not send sensitive information to email accounts other than on-campus accounts. Use an authenticated method of distribution when on-campus accounts are not available.
- Always use an authenticated and approved protocol for remote communication when accessing critical servers or resources containing personal or confidential information. Use the campus VPN when accessing any critical servers such as administrative systems (CMS) from off campus.
- Get appropriate authorization before taking University equipment off-site.

Maintain:

Maintain confidentiality, integrity, and access measures up-to-date. Securely dispose of unnecessary confidential information in an approved manner.

- Remove any confidential and private information that it is no longer needed. This will minimize the liability in case the computer becomes infected or compromised.
- Ensure that confidential, sensitive, or personal data is properly cleansed from internal disks or removable media prior to disposal or transfer to others. Seek authoritative advice on disposing of equipment and data.

4.0 Recommended Practices for Managers

Vice Presidents, College Deans, Directors and Department Heads, with guidance and assistance from the Information Security Office, should identify, protect, communicate, and maintain all confidential information under their responsibility.

Decentralized computing systems that contain Level 1 and Level 2 information are subject to periodic assessments by the Information Security Office to ensure compliance with the CSU Information Security Policies and Standards.

Identify:

Identify and inventory all systems containing, processing, or transmitting confidential information.

Protect:

Protect confidential information by allocating appropriate resources, granting appropriate access to information, supervising operations concerning confidential information, and maintaining operations concerning the integrity of that information.

- Protect confidentiality and security of electronic and printed information (paper) maintained in work areas.

- Ensure the authorized access and use of information systems and repositories that contain or process confidential information.
- Provide employees with appropriate resources to secure information systems and repositories where confidential information is processed, stored, or handled.
- Grant employees only the appropriate level of access necessary for them to work with confidential data.
- Maintain appropriate records of authorized access to confidential data.
- Provide adequate resources for the continuation of training and education for all employees under their responsibility with access to confidential information.
- Ensure all employees complete the online Information Security Training course prior to gaining access to information systems and repositories containing Level 1 and Level 2 information.
- Ensure all systems require a user id/password, which must adhere to the recommendations within the CSUSB Access Controls Standard.
- Ensure doors to file rooms, including dual use rooms, used to store sensitive paper documents are locked at all times, and access to the rooms are limited to only those individuals with a demonstrated need for access.
- Ensure file cabinets used to store sensitive paper documents are locked after business hours.

Communicate:

Communicate management's responsibility to protect the privacy rights of University faculty, staff, students, and partners and to ensure compliance with all legal and policy requirements.

Communicate the responsibility and expectation to employees under their supervision to follow appropriate procedures for the protection of confidential information.

Promptly report any possible unauthorized access, use or loss of information or an information system to the Information Security Office.

Develop and Implement:

Implement and administer standards and practices based upon these recommendations.

Develop, implement, and communicate plans and procedures for...

- ...maintenance and management of the software environment and applications on each for the systems under their responsibility which contain, access, transmit or process confidential information.
- ... verification that background checks are conducted for new hires with access to confidential data or systems.
- ...retention of electronic and printed material records containing confidential information.

- ...destruction of electronic records and printed materials containing confidential information. (Destruction must be thorough to prevent unauthorized access to confidential information.)
- ... identifying and prioritizing, based on duration of downtime and severity of impact to operations, critical systems under their responsibility.
- ...preservation of information in the event of natural or man-made disasters
- ... Business Continuity and Disaster Recovery for ALL critical systems under their responsibility. (It is unpredictable when critical systems may have a hardware failure, they may become compromised and must be removed from the network, or they may be destroyed or damaged in the case of a disaster.)
- ...notifying the Information Security Office when new systems containing or establishing ongoing access to confidential information are developed, whether within the confines of the department/office or placed on the campus network
- …the disposal of all electronic data records in accordance with the recommended CSU and CSUSB retention schedule.

Renew awareness of recommended practices for safeguarding confidential information expectations periodically. (No less than annually).

Define functions and approve authorization for staff members who need access to confidential data.

Maintain:

Maintain inventories and confidentiality, integrity, and access measures up-to-date. Securely dispose of unnecessary confidential information.

- Maintain an up-to-date registry of all systems containing confidential information.
- Conduct an annual information risk assessment on all systems containing confidential information, and critically evaluate the adequacy of existing safeguards and compliance with campus safeguarding policies and procedures.
- Maintain appropriate and timely documentation and training for employees under their supervision with access to confidential data.
- Ensure that procedures have been adopted for upgrading and updating the information systems when critical security software updates are released.
- Ensure the information systems are managed and administered following recommended security practices.
- Campus departments will submit a periodic report to the Information Security Office of their registry of Level 1 and Level 2 data maintained in electronic and paper files.
- Deletion of any protected data on disposed computers must be documented by the department.
- All backup tapes of critical systems and data must be stored in a secure off-site facility and system backups that contain protected data must also be encrypted.

- Campus departments must perform periodic reviews of user access privileges to information systems and repositories where sensitive data is processed, stored and handled. Proof of the review (i.e., a manager approval via email) must be submitted to the Information Security Office.
- Ensure that all server room doors are locked at all times, and either video cameras or after-hours alarm systems are installed.
- Remove access to the server rooms from individuals who do not have a demonstrated need for access.
- Periodically re-certify the list of individuals authorized to access the server rooms.
- Install appropriate fire extinguishers in all server rooms.
- Remove from server rooms all combustible materials, obsolete equipment, and other items that are frequently used by non-IT personnel.

Level 1: Confidential

- Strong consideration should be given to encrypting this data while in storage. Confidential data should always be encrypted when traversing a public network (e.g. Internet) or when traveling between CSUSB locations.
- Confidential Personal Identifiable Information (PII) should be encrypted when in transit and storage.

Level 2: Internal Use Only

- Information should always be encrypted when traversing a public network or when traveling outside the CSUSB private network.

5.0 Required Disclosure of Security Breach

The University is required to disclose any breach of system security to California residents whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

Any university student, faculty, staff, consultant or any other person, employed by CSUSB or any auxiliary CSUSB organization, having access to CSUSB confidential information must immediately notify their immediate supervisor and the Information Security Office when they have any reason to suspect that such a breach has occurred.

The Information Security Office will provide assistance and follow pre-established and appropriate procedures to ensure that the campus complies with applicable laws regarding notification of security breaches involving confidential information.