Protecting Confidential Data

Security of confidential data is of utmost importance at CSU, Chico. By law, most student and employee information is confidential and must be handled in a secure manner. No private/confidential data should be stored on your computer or in unlocked areas.

Information kept on your computer can be accessed by someone using your computer or hacking into it from the outside. When the security of personal information is believed to be breached, hundreds of hours of university and outside staff time are involved in investigating and repairing the breach and notifying those affected.

You are responsible for the security of the material that you store, send, or display using the campus computing and communications resources. If you work with confidential information you must be aware of and comply with numerous legal requirements and policies.

This information below was excerpted from The Data Classification and Protection Standards document found on the Information Security website.

What is Protected Information?

"Protected information" is an umbrella term for information that is linked to an individual person’s identity, such as Social Security numbers, drivers’ license data, and credit card or bank account information (sometimes called Personally-Identifiable Information, or PII) and which can be used to facilitate identity theft. Universities in particular have become attractive targets for hackers because of the freedom with which information is exchanged in an educational environment. Chico State University, like other institutions, is legally required to be vigilant and proactive in the protection of PII that’s been entrusted to us. Learn more about the steps CSU, Chico takes to protect the confidential data stored on its networks (http://www.csuchico.edu/isec/data_protection.shtml).

Data Classification and Protection Standards

Data Classification and Protection Standards (www.csuchico.edu/isec/data-classification-protection-standards.pdf) have been developed by CSU, Chico to classify various types of information as outlined below:

Level 1 protected data: Confidential information governed by existing law or statute such as Social Security numbers and names, credit card numbers with cardholder names, or medical records related to an individual. Level 1 data includes PII (social security numbers, credit card numbers, driver’s license numbers, etc.) as well as medical records, passwords, and sealed bids.

- Passwords or credentials that grant access to level 1 and level 2 data
- PINs (Personal Identification Numbers)
- 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, and 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
- Biometric information
- Electronic or digitized signatures
- Private Key (digital certificate)
- Law enforcement personnel records
- Criminal background check results
- EMEDC records
- Prospective donor profiles
- Retention Tenure & Promotion Documents (RTP)
Level 2 private data: Internal use information that must be protected due to ethical or privacy concerns such as student grades, courses taken, or disciplinary actions.

- Identity Validation Keys (name with)
  - Birth date (full: mm-dd-yy)
  - Birth date (partial: mm-dd only)
- Photo (taken for identification purposes)
- Student Information: Educational Records not defined as “directory” information, typically:
  - Grades
  - Courses taken
  - Schedule
  - Test Scores
  - Advising records
- Vulnerability/security information related to a campus or system
- Campus attorney-client communications
- Mother’s maiden name
- Race and ethnicity
- Parents’ and other family members’ names
- Birthplace (City, State, Country)
- Gender
- Marital Status
- Employee Information
  - Employee net salary
  - Home address
  - Personal telephone numbers
  - Personal email address
  - Payment History
  - Employee evaluations
  - Pre-employment background investigations
  - Educational services received
  - Disciplinary actions
  - Student photo
- Library circulation information.
- Trade secrets or intellectual property such as research activities
- Location of critical or protected assets
- Licensed software
- Physical description
- Other

Level 3 public (not protected) data: General information such as a person’s title, email address, or other directory information that is available in the public domain.

Campus Identification Keys
- Chico State ID (EmpID)
- User ID (do not list in a public or a large aggregate list, protection of SPAM, where it is not the same as the student email address)

Student Information
- Educational directory information (FERPA)

Employee Information
- Employee Title
- Employee work location and telephone number
- Employing department
- Employee classification
- Employee gross salary
- Name (first, middle, last) (except when associated with protected information)
- Financial budget information
- Signature (non-electronic)

Action Items for keeping the confidential information you have and use protected.
1. Use campus provided tools to help locate, protect, or delete confidential Level 1 protected data stored on University computers.
2. Delete all unneeded confidential information from your files or computer; then empty computer trash can or recycle bin.
4. Password protect confidential documents, such as Excel spreadsheets, Word documents, etc.
5. Avoid becoming a victim of phishing scams. Stop and think any time you find yourself tempted to click on a link in an email. If it looks suspicious, delete it. More information on spam/phishing scams is available here: http://www.csuchico.edu/isec/basics/spam-and-phishing.shtml

The Information Security (www.csuchico.edu/isec) Office takes the protection of our campus assets seriously and you can find a lot of information on their website, including:

- Information Security Basics - (www.csuchico.edu/isec/basics/index.shtml)

It is everyone’s responsibility to protect university information.