




California
State
University,
Fresno

September 24, 2008

Memorandum

To: Managers

From: John D. Welty 
President

Subject: Confidentiality of Data

In March 2006, I asked for your help addressing the growing challenge of maintaining the confidentiality of our information (paper and electronic). The data we use in our normal course of business is now even more vulnerable to theft than it was a few years ago. The expanded use of mobile devices (e.g., laptops, PDAs, smart phones, thumb drives) to store university data has made access to data easier and increased the likelihood of theft or loss (due to the mobility of these devices). Should this data fall into the wrong hands, the privacy of our faculty, staff and students may be violated.

I'm sure you have seen the numerous headlines about the theft of confidential data and the resulting impact to institutions. You may not be aware our institution has also been affected. Since I last wrote to you regarding this matter, we have experienced multiple isolated incidents where mobile devices containing confidential data were lost or stolen. These devices, whether they are in a hotel room, a parked car or in your office, are popular targets of theft and can easily disappear quickly. The loss or theft of a mobile device containing confidential information can have serious consequences for the University and the individuals affected. There is little doubt the use of mobile devices can enhance our effectiveness, but their use requires additional safeguards and diligence.

In 2006, each organizational unit was asked to develop a plan requiring specific attention to the following items:

- Each organizational unit should develop a written plan for safeguarding confidential information in your area, including:
 1. name of the office, department, or operation where confidential information is handled;
 2. justification for keeping confidential information (outside of secure administrative information systems);
 3. specific positions using confidential information and validation that the confidential information is necessary to perform job functions;
 4. administrative controls implemented to ensure appropriate individuals/positions have access to confidential information;
 5. description of methods for retaining and physically securing confidential records;
 6. description of methods for destruction of confidential records; and
 7. description of training provided to employees who handle confidential data including content, frequency, delivery method, etc.

Office of the
Vice President
for Administration and
Chief Financial Officer

5241 N. Maple Ave. M/S TA52
Fresno, CA 93740-8027

559.278.2083
Fax 559.278.2928

- Employees under your supervision, including student assistants, should know what is considered "confidential data" and what is considered "personal data that can lead to identity theft." (See attached Confidential and Personal Data Elements.)
- Employees under your supervision, including student assistants, should complete the appropriate online security awareness training which will be offered in the fall of 2006. The curriculum is currently under development and will include separate courses for the basic user, MPPs and those who primarily work in technology positions.
- Take reasonable steps to secure all confidential and personal data used by employees under your supervision, including student assistants, that can lead to identity theft.
- Electronic files containing confidential data and personal data that can lead to identity theft are kept on University servers, not individual laptops or temporary storage devices. If it is necessary for the operational needs of your unit to keep these data on temporary devices, precautions should be taken to secure the devices, and remove the data as soon as possible.
- No such data should leave your work area without your knowledge and approval.

To reduce our risk, I am requiring each organizational unit to update their plan for safeguarding confidential information to include a section addressing the use of mobile devices. This section should include the following information:

- A definitive statement on the use of mobile devices (e.g., laptops, PDAs, smartphones, mobile storage, thumb drives, DVDs, CD) for storage of confidential data. If any mobile devices are authorized for confidential data, even on a temporary basis, the plan should contain:
 1. The name of the individual, device type and justification for this person to carry confidential data. Examples:
 - Jane Doe uses a laptop to store data needed to work from home and telecommutes on a regular basis.
 - John works in an off-campus office and regularly carries a mobile hard drive containing confidential information between campus and the off-campus location.
 - Dr. X has a roster of student addresses he keeps on a thumb drive so that he can perform mail merges and email distribution from his home computer.
 2. Description of how the data is protected. Where possible, information should be protected physically or through encryption and passwords. Examples:
 - John Smith uses the University standard encryption software (TrueCrypt is available from ITS) to encrypt all of the data on his thumb drive.
 - Jan Adams stores all of her confidential information in an encrypted file folder, using File Vault, on her Mac notebook and access requires a strong password.
 3. Describe the alternate storage of the data stored on mobile devices. Mobile devices should not be the sole location of University data. Due to the increased risk of theft or loss of these devices, copies or backups of University data from these devices are more critical than backups of data stored centrally. Examples:
 - Dr. Johnson regularly backs up the contents of her encrypted thumb drive to the secure departmental server just in case the thumb drive is stolen.
 - Pamela Clark uses synchronization to make sure that her encrypted file folder on her notebook is copied to the central and secure file services.

4. Describe the awareness training authorized individuals receive and how often the training is refreshed. Examples:
 - Our department semi-annually reviews our data confidentiality plan, describes best practices to our faculty, and demonstrates the use of several key technologies.
 - All users of confidential data have taken the on-line security awareness training and we review it on an annual basis.
5. Describe the process you follow should confidential information be lost or stolen. Examples:
 - We notify campus PD, our VP and ITS as soon as we realize the loss.

Your update to the written plan must be completed and submitted for review by the appropriate vice president no later than November 30, 2008.

Thanks for your prompt attention to this important topic.

JDW:rb

Confidential and Personal Data Elements September 24, 2008

Confidential Information means any information, including computerized data, identified in governing law, regulation, or policy as individually identifiable health information, education records, personally identifiable information, non-public information, non-public personal data, confidential personal information or sensitive data.

Examples of state and federal regulations that require protection of data or combinations of data maintained at the University:

- California Information Practices Act of 1977 (California Civil Code, section 1798)
- Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability & Accountability Act of 1996 (HIPPA)
- Gramm-Leach-Bliley Act of 1999

Examples of data that is considered confidential:

- Social Security Number
- Education Records
 - Educational Activities and Sports (official)
 - Educational Attendance Dates
 - Educational Degrees
 - Educational Enrollment Status
 - Educational Grade Level
 - Educational Major Field of Study
- Number of Tax Exemptions
- Amount of Taxes Withheld
- Amount of OASDI Withheld
- Marital Status
- Voluntary/Involuntary Payroll Deduction/Reductions (amount and types)
- Survivor's Amount
- Net Pay of Employee
- Home Address
- Home Telephone Number
- Birth Date or Partial (Month-Day)
- Birthplace
- Ethnic Data
- Designee for Last Payroll Warrant
- Gender Data
- Veteran Status
- Performance Evaluations
- Disciplines
- Drivers License Number
- California Identification Number
- Credit Card Number
- Debit Card Number
- Financial Account Number
- Payment History
- Medical Records
- Psychiatric Records
- Mother's Maiden Name
- Full Name (First Middle Last)
- Parents or Other Family Members Names
- Passwords
- Pins