CSU San Marcos   Confidential Data Survey

Introduction

New CSU-wide policies and standards require us to maintain an inventory of our critical or "protected" information assets. The CSU developed a data classification standard which categorizes information into three levels. Level 1 data is considered "confidential" and generally consists of information that is protected by law such as Social Security Numbers, payment card information and health records. Level 2 data is considered "internal use" and generally consists of information that is private and is protected due to proprietary, ethical or privacy considerations.

Purpose

The purpose of the survey is to determine how your department collects, processes, transmits, and stores "protected" data. Appendix A contains further description of protected data.

Instructions

Please provide information about "protected" data that you store. The CSU has identified two levels of protection for data - "Level 1" is generally the kind of information protected by laws that limit the use of the data. Examples include Social Security Numbers, payment cards, driver's licenses, medical records. "Level 2" data includes information that must be protected for privacy or ethical concerns. Examples include private student and employee information. Where you are uncertain how to classify the data you use, please contact me (x4779 or jhumes@csusm.edu) or describe it on this form as "other" and we will work together to determine how it should be classified. If you do not use the types of information listed, please write "N/A" in the "Comments" field.

Please note that you do not need to identify:
- CMS data unless that protected data is downloaded and stored on campus.
- Stored hardcopy versions of travel or other employee forms,
- Procard records

CSU San Marcos   Confidential Data Survey

Instructions

1. Complete **all sections** of the form.
2. Return completed form to Teresa Macklin (macklin@csusm.edu, x4787)

		Today's Date	
Contact Information			
Full Name		**Title**	
Department		**Phone Number**	
Manager's Full Name			
Questionnaire			

1.	**Do you *create, collect, and/or process (which includes use or have access to)* the following types of Level 1 data?**		
	Passwords or credentials	☐ Yes	☐ No
	PINs (Personal Identification Numbers)	☐ Yes	☐ No
	Birth date combined with last four digits of Social Security Number (SSN) and name	☐ Yes	☐ No
	Credit card numbers and security codes with cardholder name	☐ Yes	☐ No
	Tax ID with name	☐ Yes	☐ No
	Driver's license number, state identification card, and other forms if national or international identification (such as passports or visas, etc.) in combination with name	☐ Yes	☐ No
	Social Security Number and Name	☐ Yes	☐ No
	Health insurance information	☐ Yes	☐ No
	Medical records related to an individual	☐ Yes	☐ No
	Psychological counseling records related to an individual	☐ Yes	☐ No
	Bank account or debt card information in combination with any required security code, access code, or password that would permit access to an individual's financial account	☐ Yes	☐ No
	Biometric information	☐ Yes	☐ No
	Electronic or digitized signatures	☐ Yes	☐ No
	Private key (digital certificates)	☐ Yes	☐ No
	Vulnerability/security information related to a campus, CO, or system	☐ Yes	☐ No
	Attorney/client communications	☐ Yes	☐ No
	Legal investigations conducted by the University	☐ Yes	☐ No
	Third party proprietary information per contractual agreement	☐ Yes	☐ No
	Sealed bids	☐ Yes	☐ No
	Other, please list	☐ Yes	☐ No

If you have answered "NO" to <u>all</u> the above items, please skip to Question #10.

2.	If you answered "YES" to any of the items in Question 1, please indicate what method(s) you use to *collect, receive, and process* Level 1 data? Choose all that apply.		

☐ CDs/diskettes
☐ Hard copy reports
☐ E-mail

☐ On the network server in a designated shared drive or folder
☐ Faxes
☐ Other, please list

3.	Do you have a *need* to store Level 1 data you collect?	☐ Yes	☐ No
4.	Do you *destroy* and/or *dispose* the Level 1 data you collect and/or process? If yes, please indicate the method you use to destroy and/or dispose Level 1 data.	☐ Yes	☐ No

5.	If you do not destroy and/or dispose the Level 1 data, *where* is the data stored? Choose all that apply.		

☐ On CDs/diskettes
☐ On my campus-issued laptop machine
☐ On my campus- issued desktop/workstation machine
☐ On my personal desktop/workstation and/or laptop machine
☐ On an external portable drive (e.g. USB flash drive, thumb drive, or external hard drive)
☐ On the network server
☐ On a shared drive
☐ On my E-mail messages
☐ At an off-site location on a backup tape or drive
☐ Other, please list

6.	Do you *retain* any Level 1 data?	☐ Yes	☐ No
7.	Do you *share* Level 1 data?	☐ Yes	☐ No
8.	If you do share, *who* do you share Level 1 data with? Choose all that apply.		

☐ Off campus or external organizations, please specify
☐ Auxiliary
☐ Other CSU organizations
☐ Other campus departments
☐ Others, please specify

9.	If you *share*, choose the method(s) that you use.		

☐ On a CD using postal services (e.g. USPS, UPS, Fedex, etc.)
☐ Hard copy reports using postal services (e.g. USPS, UPS, Fedex, etc.)
☐ On the network server in a designated shared drive or folder
☐ Via E-mail
☐ Via external portable drives (e.g. USB flash drive, thumb drive, or external hard drive)
☐ On a CD/diskettes stored on campus
☐ Hard copy reports stored on campus
☐ Other, please list

10.	Does your department do any one or more of the following, including?		
	Accept credit or debit cards for face-to-face (in-person) sales?	☐ Yes	☐ No
	Accept credit or debit cards for e-commerce sales (over the internet)?	☐ Yes	☐ No
	Accept credit or debit card for fax transmission or phone transmission sales?	☐ Yes	☐ No
	Store, process, and/or transmit credit or debit card information in any form (paper or electronic) that relates to or contains the Primary Account Number information?	☐ Yes	☐ No

CSU San Marcos   Confidential Data Survey

Appendix A

In order to protect information from unauthorized disclosure, use, modification or deletion, all data, whether electronic or in print, uses the following designated information classification system as identified in the [Systemwide Information Security Standards](#).

Classification	Description	Examples
Level 1 Confidential	Confidential Information is information maintained by the University that is exempt from disclosure under the provisions of the California Public Records Act or other applicable state or federal laws. Confidential information is information whose unauthorized use, access, disclosure, acquisition, modification, loss, or deletion could result is severe damage to the CSU, its students, employees, or customers. Financial loss, damage to the CSU's reputation, and legal action could occur. Level 1 information is intended solely for use within the CSU and limited to those with a "business need-to-know." Statutes, regulations, other legal obligations or mandates protect much of this information. Disclosure of Level 1 information to persons outside of the University is governed by specific standards and controls designed to protect the information.	• Passwords or credentials • 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 debt 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) • Vulnerability/security information related to a campus or system • Attorney/client communications • Legal investigations conducted by the University • Third party proprietary information per contractual agreement • Sealed bids
Level 2 Internal Use	Internal use information is information which must be protected due to proprietary, ethical, or privacy considerations. Although not specifically protected by statute, regulations, or other legal obligations or mandates, unauthorized use, access, disclosure, acquisition, modification, loss, or deletion of information at this level could cause financial loss, damage to the CSU's reputation, credibility, violate an individual's privacy rights, or make legal action necessary. Non-directory educational information may not be released except under certain prescribed conditions.	**Identity Validation Keys (name with)** • Birth date (full: mm-dd-yy) • Birth date (partial: mm-dd only) **Student Information-Educational Records** (Excludes directory information) including: • Grades • Courses taken • Schedule • Test Scores • Advising records • Educational services received • Disciplinary actions Non-directory student information may not be released except under certain prescribed conditions **Employee Information** Including: • Employee net salary • Employment history • Home address • Personal telephone numbers • Personal email address • Payment History • Employee evaluations

		• Background investigations • Mother's maiden name • Race and ethnicity • Parents and other family members names • Birthplace (City, State, Country) • Gender • Marital Status • Physical description • Photograph **Other** • Library circulation information. • Trade secrets or intellectual property such as • research activities • Location of critical or protected assets • Licensed software
Level 3 Public	This is information that is generally regarded as publicly available. Information at this level is either explicitly defined as public information or intended to be available to individuals both on and off campus or not specifically classified elsewhere in this standard. Knowledge of this information does not expose the CSU to financial loss or jeopardize the security of the CSU's information assets. Level 3 information may be subject to appropriate campus review or disclosure procedures to mitigate potential risks of inappropriate disclosure. Publicly available data may still subject to appropriate campus review or disclosure procedures to mitigate potential risks of inappropriate disclosure.	**Campus Identification Keys** • Campus identification number • User ID (do not list in a public or a large • aggregate list where it is not the same as the student email address) **Student Information** • Educational directory information (FERPA) **Employee Information (including student employees)** • Employee Title • Status as student employee (such as TA, GA, ISA) • Employee campus email address • Employee work location and telephone number • Employing department