California State University, Fresno

Information Protection Plan

August 18, 2011

REVISION CONTROL

Document Title: Information Protection Plan

Date	By	Action	Pages
08/01/2011	Rafael Villegas, Ph.D.	Created Information Protection Plan	All
08/09/2011	Rafael Villegas, Ph.D.	Edits	6,7,8
08/18/2011	Rafael Villegas, Ph.D.	Edit	33

Review/Approval History

Date	By	Action	Pages

Table of Contents

1.0 Introduction

1.1 Summary

California State University, Fresno relies extensively on data and information technology to execute its mission and provide services to students, faculty, staff and the surrounding community.

Information security is integral to the business and academic functions of the university. Fresno State must manage its data and information resources with due diligence and take the necessary steps to appropriately safeguard them while complying with state and federal laws, regulations and policies.

This *Information Protection Plan* specifies information security measures to preserve the confidentiality, integrity and availability of Fresno State data and information resources.

1.2 Purpose

Departments and units were previously required to develop and complete their own separate data confidentiality protection plans.

Instead of individual protection plans, the Information Security Office has developed the *Information Protection Plan* that provides for a common framework. Organizational units can utilize this plan as a template to ensure a consistent approach to the implementation of information security practices to safeguard university resources and data, whether on paper or electronic format.

Each department including auxiliary units, to indicate conformance of their respective area with the *Information Protection Plan*, need to complete and sign the information protection forms:

- Self assessment (Appendix A)
- Inventory (Appendix B)
- Media Protection (Appendix C)
- Reuse, retirements and destruction (Appendix D)

These forms are sheets in a Microsoft Excel document, which is available from the Help Desk (https://help.csufresno.edu) web site under the staff and faculty forms section.

Departments and units must attach a signed and dated statement of any exceptions, additions or modification of the *Information Protection Plan* for their respective area.

1.3 Scope

The safeguarding of Fresno State's data and information resources is integrated into its business and academic operations. Therefore, the safeguards, procedures and processes outlined in the plan apply to all:

- University departments, including auxiliary units and organizations that provide articles or services to Fresno State
- Students, faculty, staff and consultants employed by Fresno State or any individual or entity with access to Fresno State data or information resources
- Categories of data (information), regardless of the medium in which the information is held (e.g. paper, electronic, oral, etc.)

2.0 Policy Management

2.1 Policy Summary

Fresno State has established information security policies based on the existing state and federal laws, regulations, policy, and California State University executive orders.

The *Data Classification Policy*, approved in August 2009, defined three classification categories (Confidential, Restricted, Unrestricted) to maintain appropriate protection of data.

The policy also requires that all institutional data possessed or used by a particular organizational unit within the university must have a designated information owner (section 4.2.4).

The *Data Handling Standard*, approved in February 2010, established several data handling requirements, for each classification category, to appropriately safeguard the information.

All existing laws (Federal and State) as well as University regulations and policies apply, including not only those laws and regulations specific to computers and networks, but also those that may apply generally to personal conduct.

The following sections provide a summary of some of the laws, regulations, executive orders and information security policies applicable to the university. It is not a comprehensive list of information security obligations.

2.2 Federal and State Regulations

- USA Patriot Act (P.L. 107-56), October 2001
- Gramm-Leach-Bliley Act of 1999: Federal Trade Commission Regulations. The Act includes two regulations: *The Financial Privacy Rule* and *The Safeguards Rule*
- Health Care Portability and Accountability Act of 1996 (HIPAA)-Final Rule
- Family Education and Privacy Act of 1974 (FERPA)
- Federal Copyright Law
- Federal Computer Fraud and Abuse Act of 1986
- State of California Information Practices Act of 1977 (Civil Code Section 1798 et seq.)
- State of California Education Code, Section 67100 et seq.
- State Of California Penal Codes, Section 502
- State of California Public Records Act (Gov. Code Section 6250 et seq.)
- California Code of Regulations, Title V, Sections 42396 through 42396.5 Privacy and Personal Information Management

2.3 California State University Policies, Executive Orders and Coded Memorandum

- California State University (CSU) Executive Order 1031: February 27, 2008, Systemwide Records/Information Retention and Disposition Schedules Implementation – Executive Order No. 1031
- CSU Executive Order 999: March 7, 2007, Illegal Electronic File Sharing and Protection of Electronic Copyrighted Material – Executive Order No. 999

- CSU Coded Memo: HR 2005-16, April 8, 2005, Requirements for Protecting Confidential Personal Data: Updated to Include Information Practices Act Web Site and Security Breach Disclosure Requirement
- CSU Coded Memo: HR 2003-23, November 19, 2003, New Legislation Regarding Use of Social Security Numbers
- CSU Memo, Increased Security Measures for CMS, March 26, 2003
- CSU HR 2003-14, HIPAA Regulations – Privacy Compliance
- CSU Information Security Policy (CSU Administrative Manual)
- CSU Records Access Manual, February 2003
- CSU Memo, Information Security Clarification, March 28, 2003
- CSU Memo, Compliance with the Gramm-Leach-Bliley Act-Safeguarding Confidential Personal Data, May 21, 2003

2.4 Fresno State Information Security Policies, Standards and Procedures

- Found at www.csufresno.edu/technology/policies/index.shtml
  - Interim Acceptable Use Policy Of Information Technology Resources
  - Data Classification Policy
  - Data Handling Standard
  - Minimum Security Baseline For Connected Devices
  - Network Connection Policy
  - Electronic Resources Emergency Response Policy (i.e. Disconnect)
  - Confidentiality of Data, President Memos of 2006, 2008, 2011

3.0 Asset Management

3.1 Policies and Standards

The university has implemented policies and procedures for the classification and protective control of data (regardless of format) and information resources.

All university information resources and data created, stored, processed or transmitted are assigned an appropriate classification and security controls in accordance with the university's *Data Classification Policy* and *Data Handling Standard*.

3.2 Risk Assessment

Risk management is the process of conducting risk assessments and implementing the agreed mitigation strategies. The university conducts regular information risk assessments to protect the availability, confidentiality and integrity of its data and information resources.

Information owners, assisted by the Information Security Office, analyze the risks and threats to data in their area and accordingly classify and oversee appropriate protection of institutional data.

The *Information Protection Plan* is updated with the results of the risk assessment.

3.3 Data Classification

The university categorizes its information resources and the data processed, stored, or transmitted in accordance with applicable laws, executive orders, policies, regulations and standards.

The overall sensitivity of institutional data encompasses its confidentiality, privacy, integrity and availability. Data with the highest risk needs the greatest amount of protection; data at lower risk can be given appropriate levels of protection. This approach allows the university to apply appropriate levels of resources to the protection of the institutional data.

All university information resources and data created, stored, processed or transmitted are assigned an appropriate classification and controls in accordance with the university's *Data Classification Policy* and *Data Handling Standard*.

Three categories (Confidential, Restricted, Unrestricted) of classification have been defined to maintain appropriate protection of university data. Confidential is the highest category (requires the highest level of protection); Unrestricted is the lowest category defined.

For each classification, several data handling requirements are defined in the *Data Handling Standard*, to appropriately safeguard the information.

Examples of data in each category are shown in Appendix E.

3.3.1 Category I: (Confidential Data)

Confidential data is highly sensitive and may have personal privacy considerations, or may be restricted by federal or state law and regulations (e.g., HIPPA, Sarbanes-Oxley, Gramm-Leach-Bliley). In addition, the negative impact on the university should this data be incorrect, improperly disclosed, or not available when needed is typically very high.

Category I data must be controlled from creation to destruction, and access will be granted only to those persons affiliated with the university who require such access to perform their job, or to those individuals

permitted by law. Access to confidential data must be individually requested and then authorized by the information owner who is responsible for the data.

3.3.2 Category II: (Restricted Data)

University data not otherwise identified as Category-I data, but which is releasable (e.g., contents of specific email, date of birth, salary, etc.) must be appropriately protected to ensure a controlled and lawful release.

University records (data) releasable under public access to government records laws is categorized as restricted data and authorized for release by the designated university custodian of records.

3.3.3 Category III: (Unrestricted Data)

University data not otherwise identified as Category-I or Category-II data is generally regarded as publically available data. Such institutional data is defined as public information and published with no restrictions.

Publicly available data is information that can be used, analyzed and obtained without requiring the permission of the information owner data is not considered sensitive.

3.4 Asset Protection

3.4.1 Plans

University departments and units develop, maintain, document, periodically update and implement *Information Protection Plan* that describe the security controls in place or are planned for the protection of confidential and restricted data and the information resources in their respective area.

3.4.2 Inventory

University departments and units, in coordination with the Information Security Office, maintain a current inventory of all confidential and restricted data and information resources and which individuals have access to such data and information resources.

3.4.3 Retention and Disposal

Each department's retention and disposal of data is managed in accordance with the retention and disposal schedule found at http://www.csufresno.edu/adminserv/records/ as mandated by CSU executive order 1031.

4.0 Human Resources Management

4.1 Employment

The university minimizes the risk of loss or misuse of data and information resources by ensuring that security controls are incorporated into human resource management. The university:

- Documents roles and responsibilities where employees have access to confidentiality or restricted information or perform security related roles
- Ensures that security responsibilities are addressed in job descriptions
- Develops and implements procedures for the separation of employees from or movement within the university

4.2 Roles and Responsibilities

Safeguarding Fresno State's data and information resources information is everyone's responsibility. In our university environment, we deal with confidential and restricted data and information resources on a daily basis. The confidentiality and integrity of such data and resources must be appropriately protected from unauthorized disclosure and use.

In addition, specific information security roles and responsibilities have been identified or assigned to individuals or units associated within Fresno State's information security program.

4.2.1 Information Security Committee (ISC)

The Information Security Committee (ISC) develops, maintains, and annually reviews the policies and standards that define the security practices followed at Fresno State to provide for the confidentiality, integrity and availability of the university's data and information resources.

4.2.2 Information Security Office

The Information Security Office is responsible for establishing and overseeing the university's information security program and provides information security consulting assistance to all university units.

4.2.3 Third Party Providers

There is periodically a business need for Fresno State to provide a third party access to University data under a contractual agreement. In some cases, these entities have access to university data that must be appropriately protected to comply with the policies of the university and to meet the requirements of state and federal laws.

Third party providers are responsible for maintaining security controls, policies and procedures that are compliant with law, regulations, policy and procedures.

4.2.4 Information Owner

Executive Order 1031 provides for the implementation of California State University (CSU) Systemwide Records/Information Retention and Disposition Schedules.

Record/information means recording upon any tangible thing in any form of communication or representation, including letters, words, pictures, sounds, or symbols, any combination of these or other

means to engage in business, regardless of media.

The executive order also requires that each campus, for retention and disposition, designate official campus custodian(s) for each type of record. “Custodian of Records” is the term of the campus-designated department head that maintains the official/original copy of the record/information at Fresno State.

The “Custodian of Record” identified from the records and retention schedule posted at http://www.csufresno.edu/adminserv/records/ is the designated Information (Data) Owner for each respective type of data.

If a “Custodian of Record” is not identified for an area in the records and retention schedule, then the highest-ranking management personnel (MPP) of that respective area shall be designated as the Information (Data) Owner.

The information owner does not legally own the data entrusted to their care. They are instead designated members of university management who act as stewards, and who supervise the ways in which certain type of information are used and protected.

Information owners ensure that all decisions regarding the collection and use of institutional data are in compliance with the law, regulations, and with university policies and procedures and such data is appropriately protected.

4.2.5 Users

Users are all individuals that interact with university data and information resources either in a support function, by working directly with an information resource or as a recipient of university data.

Users include all university employees, students and contractors, including vendors and agents, who provide or access data, services or resources at Fresno State.

Users are aware and comply with state and federal law, Fresno State policies, standards and procedures regarding the protection of university data and information resources.

4.3 Information Security Education and Awareness

The information security education and awareness program, provided on a regular basis, ensures users are aware of their information security responsibilities, reporting of information security incidents, and the requirements for the protection of confidential and restricted data.

4.4 Privacy

Only necessary information is collected. Personally identifiable information (PII) about an individual is not collected just because that information may come in handy later. Individuals are informed about the need to collect the information and how the information will be used. It is the responsibility of any individual with access to confidential or restricted data to keep that data confidential.

5.0 Physical and Environmental Management

5.1 Filing and Markings

Confidential and restricted documents are filed with appropriate file covers and/or markings identifying their classification category.

Markings for Category I documents include a CONFIDENTIAL label. Markings for category II documents include a RESTRICTED label. No special filing or markings are required for Category III documents.

Labeled envelopes or folders appropriately identifying the confidential or restricted classification category are used in inter-campus mailing.

5.2 Clear Desk

The university has a clear desk and clear screen requirement for areas that handle confidential or restricted data.

A clear desk requires that confidential or restricted data is secured when computers are unattended and that unauthorized individuals are not able to access any confidential or restricted material.

For long periods this would mean 'logging off' from computer systems, but for shorter periods a screen saver with password or some similar desktop locking mechanism is adequate.

At close of business, lock-up procedures require that personnel:

- Quit all systems and networks and where possible shut down their computers
- Ensure that no confidential or restricted information is left unsecured
- Ensure information is disposed of lawfully
- Ensure that electronic media containing confidential or restricted data is secured
- Secure/lock offices and file cabinets containing confidential or restricted data
- Ensure that keys to facilities holding confidential or restricted data are secure

5.3 Disposal of Records (Data)

In accordance with university policy, university owned resources are sanitized and/or disposed of properly. The disposal, including the destruction, of records is performed in accordance with the university retention and schedule policy to ensure the legal, systematic, and consistent disposal of records no longer required for business, academic or other purposes.

Paper drafts, working papers, originals and copies containing confidential or restricted are shredded.

Paper drafts, working papers, originals and copies containing unrestricted data may be recycled.

5.4 Sanitization and Disposal of Electronic Media

Electronic media and information resources are sanitized and/or destroyed appropriately. The following media is shredded, pulverized or disintegrated if it contains or may have contained confidential or restricted data:

- Microfiche and microfilm
- Optical discs, including CDs and DVDs
- Printer ribbons

Other media including various forms of erasable or alterable memory, solid state or magnetic media such as hard disk drives may be sanitized for reuse by wiping or by using a suitable degaussing tool.

Sanitization of magnetic media by erasure (wiping) may be performed using specifically designed security erasure software and university approved procedures to effectively wipe the contents of electronic storage media.

5.5 Copying

Confidential or restricted data, in any form, is only to be reproduced (copied or re-printed) when it is strictly necessary and the permission of the information owner is obtained.

Copiers and printers are not left unattended if confidential or restricted data is being reproduced unless there are suitable physical access controls to prevent unauthorized persons from viewing the material being printed.

5.6 Storage

Physical security protection, in accordance to the classification of data stored in a given location, is in place for all offices, rooms and storage facilities. Building and entry controls are in place for areas that process or store confidential or restricted data.

Secure storage may range from, but is not limited to, lockable drawers, lockable file cabinets, locked offices or secure rooms.

Confidential or restricted data (electronic or paper) is stored in a locked drawer, in a locked room, or in another approved secure location and is out of sight at all times when not in use.

Confidential and restricted data on portable devices, stand-alone or portable computers, hard drives, flash memory drives, and other storage devices are treated with the same controls applicable to the storage of paper records.

6.0 Communications and Operations Management

6.1 Copyright

As the university is subject to federal law, it must comply and abide with copyright law and copyright policies. Each user must respect this copyright and must comply with published usage restrictions relating to any program, information, image, web page or other material.

6.2 Anti-Malicious Software

All network-connected devices able are required to implement controls for the prevention, detection and removal of malicious code. Malicious code includes, but is not limited to, viruses, spyware, worms, Trojan horses and logic bombs. The anti-malicious software is installed, running and up-to-date on all devices capable of running such software.

The anti-malicious software is updated with new definition files and scanning engines as soon as possible after vendors make them available. At minimum, the anti-malicious code software runs weekly scans of the entire device.

6.3 Software Authorization

Software is not downloaded and installed on information resources without appropriate authorization. Any individual who installs software and/or information on University resources must ensure full compliance with any relevant copyright requirements and licensing agreements.

6.4 Firewalls

Firewalls are implemented at the network perimeter, on the internal network, servers, computers and network-connected devices.

All network-connected devices (laptops, workstations, etc.) able are configured to enable the built-in (native) firewall of the device or a more advanced firewall is active.

Firewall configurations permit and allow for policy compliance verification and vulnerability scanning by the Information Security Office.

The defined firewall rules on these information resources match network access requirements.

6.5 Backup and Recovery

Backup frequency is based on business risks, however backups of the operating system and applications are at a minimum on a quarterly basis.

Backup restoration procedures are documented and available to those that requires the information.

At least one copy in each backup cycle and restoration procedures is stored off-site and in accordance with the business continuity and disaster recovery plans.

Regular tests are performed to ensure the backup procedures meet the requirements of business continuity and disaster recovery plans.

Backup information is afforded appropriate controls, including physical and environmental, commensurate with the security classification of the data or information resource.

6.6 Transmission

6.6.1 Verbal

Discussions of confidential or restricted information occur behind closed doors and/or care is taken to ensure that people without a need to know are not able to overhear discussions.

6.6.2 Facsimile

Confidential and restricted faxed documents are appropriately labeled to state the confidential nature of the communications and include instructions should the fax be misdirected.

If possible, arrangements are made at both ends of the transmission to monitor the fax machine until the entire fax has been sent and received. Do not leave a fax machine unattended when sending or receiving confidential or restricted documents.

6.6.3 Telephone

Confidential or restricted data is not be left on voice mail messages unless it is a business requirement or at the request of the recipient. Confidential or restricted data is not forwarded to another voice mail.

6.6.4 Electronic

Email is an important tool for information exchange but information included in emails often traverses public and untrusted networks such as the Internet. Sending unencrypted confidential or restricted data over email is avoided.

All confidential and restricted data and authentication credentials transmitted via wired, video, wireless or cellular networks (e.g. email, instant messaging, file transfers, web applications, etc.) utilizes an encryption mechanism between the sender and receiver; and the file, document, email, or folder is encrypted before transmission.

7.0 Access Management

7.1 Access Controls

All confidential or restricted data and information resources capable of, have authentication and access controls to ensure that only authorized users can access the data and information resource and it is not improperly disclosed, modified, deleted or made unavailable.

7.2 Authentication

The controls to restrict logical access to data and information resources limit user access on the basis of need-to-know, provide users with the minimum of privileges required for their job and require requests for access to confidential or restricted data or information resources to be authorized by the information owner or other approval authority.

Where practical, server, computer and communications equipment is located in secure areas with access control mechanisms required to restrict use to authorized personnel only.

7.3 User Access

The user's manager authorizes access rights before a user is granted access to the confidential or restricted data or information resources. Where applicable, access control mechanisms (passwords, two factor authentication, etc.) are used to restrict access to all computer systems, including hardware, software and confidential or restricted data.

User authentication requires a unique identifier (user ID) and the unique user ID's is not reassigned when no longer needed.

Passwords used to authenticate a users access to confidential or restricted data follow these best practices for password protection:

- Strong passwords are always used
- Passwords are never shared with anyone
- Passwords are changed periodically (at minimum every semester)
- Passwords are changed immediately if they have been compromised
- Different passwords are used for all user accounts

A strong password is at least eight characters long and contains upper and lower case letters, numerals, and symbols found on the keyboard. If passwords must be written down on a piece of paper, store the paper in a secure place and destroy it when it is no longer needed.

Changes in an employee's duties are reflected in their access control rights. Changes are carried out on a timely basis. Access privileges are disabled or modified when users change jobs, or leave the university permanently or are on leave for a prolonged period.

User access rights are subject to regular review using a formal process.

Special privileges are restricted and controlled. Special privileges include privilege users (i.e. administrator/root access), security administration and database administration.

Privileged access to information resources is used only when necessary to perform job duties and only for activities requiring privileged access.

All users with privileged access to data and information resources have signed a confidential access agreement and the agreement is filed with the appropriate manager (MPP).

Users follow their responsibilities with regard to system access including securing unattended information resources and data and keeping a clear desk.

7.4 Network Access

All devices connecting to the Fresno State Network register and are configured not to conflict with centrally provided services. Registration of the device, at minimum, identifies an appropriate contact for the device connecting to the network. Periodic registration renewal is necessary to maintain up-to-date information of the devices connected to the network.

7.5 Remote Access

External information resources that are used to administer university information resources or access confidential or restricted information are secured and configured in accordance with all relevant university policies and procedures.

Documentation of all individuals with remote access to university confidential and restricted data or that administer information resources is maintained to minimize security risks.

7.6 Audit Logs

An audit logging process is implemented to maintain the confidentiality and integrity of data and information resources. The audit logs are capable of providing information, which can be used to investigate inappropriate or illegal access.

Exceptions and information security events are produced, maintained and monitored.

Audit logs are maintained for a minimum of 90 days or as required by retention schedules.

Server and computer administrators do not have write, modify or delete access to audit logs. This restriction reduces the risk of unauthorized access and protects the administrator.

8.0 Systems Acquisition, Development and Maintenance

8.1 System Security Requirements

Security requirements and specifications are addressed in the initial stages of development for any new or upgraded information resources containing confidential or restricted data. These requirements identify and address any potential security risks and vulnerabilities.

8.2 System/Application Files

Operational software is to be maintained at a level supported by the vendor and to the latest patch level possible after appropriate testing, planning and migration control measures have been carried out when upgrading, patching or installing new software versions to ensure the overall security of the system.

8.3 Cryptographic (Encryption) Controls

Cryptography (encryption) can be used to secure data and when used within an appropriate network protocol can provide an encrypted and trusted communications. Advancements in computing power give encryption algorithms a finite lifetime. Therefore, the use of appropriate key lengths and key strengths provide an appropriate level of protection based on the classification category of the data or information resource.

8.3.1 Servers

Unless servers are in a secure dedicated server room with physical access control, all confidential and restricted data is encrypted, using a university approved encryption solution.

Servers containing confidential or restricted data must be registered in a central database.

8.3.2 Workstations (End-User Devices)

All confidential and restricted data stored on workstations (i.e. computers) is encrypted using a university approved encryption solution.

8.3.3 Portable (Mobile) Devices

All mobile devices (laptops, notebook computers, handheld computers, PDAs (personal digital assistants), pagers, cell phones, etc.) able that process and/or store confidential or restricted data are encrypted using a university approved encryption solution.

8.3.4 Removable Media

All confidential and restricted data is encrypted, using a university approved encryption solution, when stored on any removable media (i.e. USB thumb drives, floppies, Compact Disk (CD)/Digital Video Disk (DVD), etc.).

8.3.5 Non-university Owned Information Resources

All confidential and restricted data is encrypted, using a university approved encryption solution, on any non-university owned information resources that is used to store or process confidential or restricted university data.

All non-owned university information resources that store or process confidential or restricted university data must adhere to all laws, executive orders, regulations, and university policies.

8.4 Vulnerability Management

Vulnerability assessments are conducted by the Information Security Office to review technical security controls and identify vulnerabilities in university information resources to properly mitigate the risk of critical vulnerabilities discovered during the assessment.

9.0 Incident Management

9.1 Event Reporting

All information security incidents are promptly reported to an appropriate manager and the Information Security Office. The reported information is used for further reviews of information security risks.

9.2 Incident Procedures

Incident procedures are in place to handle information security events effectively once they have been reported.

The Information Security Office is responsible for coordinating the handling of information security incidents.

The Director of Technology Services or designee, having the responsibility to maintain and operate the university infrastructure, has the authority to implement emergency security measures to protect university information resources.

In an emergency situation, these procedures may involve shutting off or disconnecting portions of the university network, blocking certain communication ports, implementing software and/or anti-virus updates, shutting down servers or workstations as a response to immediate threats or attacks to the university information resources.

Senior administration is notified as soon as practical of actions taken in emergencies. Those departments and units affected by such emergency actions are notified and consulted in a timely manner.

10.0 Business Continuity Management

10.1 Business Continuity

Each department has developed business continuity plans that are reviewed and tested on a regular basis.

A review of continuity plans occurs after any significant disruption to services to ensure procedures are updated to reduce the risk of a repeat occurrence.

10.2 Disaster Recovery

Each department maintains disaster recovery plans to ensure that the availability of data and services can be restored following a disaster.

The criticality of data, information resources and services is documented to determine the vulnerability of those resources and develop risk management strategies.

11.0 Compliance Management

11.1 Legal

A summary, of information security related legal requirements, is contained in this *Information Protection Plan*. However, each department must consult CSU legal counsel on specific legal requirements that may arise for their area.

11.2 Policy

Information security policies, procedures and compliance are reviewed and reported to appropriate management at least annually.

11.3 Audit

The Information Security Office periodically audits each university department for compliance with the *Information Protection Plan* to ensure appropriate security controls are maintained.

11.4 Forms

Adherence to the *Information Protection Plan* requires completion of each of the spreadsheets in the information protection form as shown in:

- Appendix A: Self assessment (i.e. conformance with *Information Protection Plan*)
- Appendix B: Inventory (i.e. authorized use and access, location, and distribution)
- Appendix C: Media Type (i.e. identification of information resources and safeguards)
- Appendix D: Reuse, Retirements and Destruction (i.e. proper disposal of data and resources)

The information protection form can be downloaded from the Help Desk (https://help.csufresno.edu) under the staff and faculty forms section.

Definitions

Access Controls – Access controls are the means by which the ability to use, create, modify, view, etc., is explicitly enabled or restricted in some way (usually through physical and system-based controls).

Authentication – The process of determining whether someone or something is, in fact, who or what it is declared to be. In private and public computer networks (including the Internet), authentication is commonly done using logon passwords.

Data (Information) – It can be printed or written on a piece of paper, stored electronically, transmitted by post or by electronic means, shown on films, or spoken in conversation. Whatever form the information takes, or means by which it shared or stored, it should always be appropriately protected. (ISO/IEC 27002:2005, page viii)

Electronic Media – Any of the following: a) Electronic storage media including storage devices in computers (hard drives, memory) and any removable/transportable digital storage medium, such as magnetic tape or disk, optical disk, or digital memory card.

Encryption – The translation of data, information or documents into a code that cannot be read without a "key". It is the conversion of data into a form that cannot be easily understood by unauthorized people.

Family Educational Rights and Privacy Act (FERPA) – A federal law that protects the privacy of student educational records.

Health Insurance Portability and Accountability Act (HIPPA) – Federal protections for personal health information held by covered entities and gives patients an array of rights with respect to that information.

Information Owner – The "Custodian of Record" identified from the records and retention schedule posted at http://www.csufresno.edu/adminserv/records is the designated Information (Data) Owner for each respective type of data. If a "Custodian of Record" is not identified for an area in the records and retention schedule, then the highest-ranking management personnel (MPP) of that respective area shall be designated as the Information (Data) Owner.

Information Resource – are devices or technologies that are designed, built, operated, organized, or maintained to process, store, transmit or output information. These information resources include, but are not limited to, voice, data and video networks, computer accounts, electronic communications, files, computing facilities, laboratories, software, and data.

Personally Identifiable Information (PII) – Information that can be used to physically locate or identify an individual, such as names, date of birth, aliases, Social Security numbers, driver's license number, biometric records, and other personal information that is linked or linkable to an individual. No single law governs all uses of personally identifiable information.

Portable (Mobile) Devices – Any transportable device that is capable of receiving and/or transmitting data. These include, but are not limited to, notebook computers, handheld computers, laptops, PDAs (personal digital assistants), pagers and cell phones.

Removable Media – Removable media devices permit data to be stored on media that is removable and interchangeable. CDs, DVDs, flash memory and floppy disks are examples of removable media.

Server –Any computer providing a service over the network. Services include, but are not limited to: Web site publishing, printing, wireless access and file sharing.

Appendix A: Self-Assessment Form

Confidential

Date:

Department Name:

Information Owner/MPP:
Information Protection Form (Part 1 of 4)

Self-Assessment

	Policy Management	Section	Y/N	Comments
1	Users are familiar with Fresno State information security polices and procedures	2.1		
	Asset Management	**Section**	**Y/N**	**Comments**
1	Risk assessment conducted	3.2		
2	Data used by department has been appropriately categorized	3.3		
3	Inventory of all confidential and restricted data and information resources	3.4		
4	Retention and disposal of data is managed as mandated by executive order 1031	3.5		
	Human Resources Management	**Section**	**Y/N**	**Comments**
1	Security controls are incorporated into human resource management	4.1		
2	Roles and responsibilities defined and users are aware of their responsibilities to protect confidential and restricted information	4.2		
3	Security education and awareness completed on a regular basis	4.3		
4	Only necessary information is collected	4.4		
	Physical and Environmental Management	**Section**	**Y/N**	**Comments**
1	Confidential and restricted documents are filed with appropriate file covers and/or markings identifying their classification category	5.1		
2	Clear desk requires that confidential or restricted data is secured when computers are unattended and that unauthorized individuals are unable to access any confidential or restricted material	5.2		
3	University owned resources are sanitized and/or disposed of properly	5.3		
4	Electronic media and information resources are sanitized and/or destroyed appropriately	5.4		
5	No unattended copying of confidential or restricted data	5.5		
6	Physical security protection for confidential or restricted data is provided in accordance to its classification category	5.6		
	Communications and Operations Management	**Section**	**Y/N**	**Comments**
1	Compliance with copyright is ensured	6.1		

3	Only authorized software is used and/or downloaded	6.3		
4	Firewall enabled on information resources with appropriate rules	6.4		
5	Backup and restoration procedures documented and tested	6.5		
6	Written process for transmission of confidential and restricted data (verbal, facsimile, telephone, electronic)	6.6		
	Access Management	**Section**	**Y/N**	**Comments**
1	Authentication is used to control access to confidential or restricted data and information resources	7.1		
2	User's manager authorizes access rights before a user is granted access to the confidential or restricted data or information resources	7.2		
3	Written process for tracking, storage and authorization of confidential and restricted data and information resources	7.3		
4	Passwords used to authenticate a users access to confidential or restricted data follows best practices for password protection	7.3		
5	Employee duties are reflected in their access control rights	7.3		
6	User access rights are subject to regular review using a formal process	7.3		
7	Special privileges are restricted and controlled, used only when necessary to perform job duties.	7.3		
8	Privileged users have signed a confidential access agreement	7.3		
9	Users follow their responsibilities with regard to system access including securing unattended information resources and data and keeping a clear desk	7.3		
10	All devices connecting to Fresno State network register	7.4		
11	External devices secured and configured in accordance with all relevant university policies and procedures	7.5		
12	Audit logs are capable of providing information, which can be used to investigate inappropriate or illegal access	7.6		
	Systems Acquisition, Development, and Maintenance	**Section**	**Y/N**	**Comments**
1	Risk assessment are conducted for new and upgraded information resources containing restricted or confidential data	8.1		
2	Operational software is maintained at a level supported by the vendor and to the latest patch level possible	8.2		
3	Appropriate encryption key lengths and key strengths are used based on the classification of the data or information resource	8.3		
4	All confidential and restricted data is encrypted on servers not in a secure dedicated server room	8.3.1		
5	All confidential and restricted data stored on workstations (i.e. computers) is encrypted	8.3.2		
6	All mobile devices that process and/or store confidential or restricted data are encrypted	8.3.3		
7	All confidential and restricted data on removable media is encrypted	8.3.4		

8	All confidential and restricted data on non-university owned information resources is encrypted	8.3.5		
9	Vulnerability assessments conducted on information resources containing confidential or restricted information	8.4		
	Incident Management	**Section**	**Y/N**	**Comments**
1	Incidents promptly reported	9.1		
2	Written incident reporting procedures	9.2		
	Business Continuity Management	**Section**	**Y/N**	**Comments**
1	Developed business continuity plans	10.1		
2	Developed disaster recovery plans	10.2		
	Compliance Management	**Section**	**Y/N**	**Comments**
1	Comply with Information Protection Plan	11.3		
2	Completed Inventory Form	11.4		
3	Completed Media Type Form	11.4		
4	Completed Reuse, Retirement, Destruction Form	11.4		
5	Completed Self-assessment Form	11.4		
Information Owner Signature*				**Date:**

***MPP** (Associate Dean, Director, or Other) Signature validates that the confidential and restricted information listed in the following sheets are necessary to perform the essential functions of the department.

Appendix B: Inventory of Data / Information Form

Confidential

Date:

Department Name:

Information Owner/MPP:

Information Protection Form (Part 2 of 4)

Identify Data

Type Of Information	Individuals Authorized To Use Or Access	Data Category (Confidential, Restricted, Unrestricted)	Legal Mandates	Authoritative Source (Yes/No)?	How Is Information Obtained?	Where Is Information Stored?	Describe How Information Is Protected In Storage?	How Is Information Shared?	Comments

Appendix C: Protection by Media / Device Form

Date:

Department Name:

Information Owner/MPP:

Information Protection Form (Part 3 of 4)

Protection By Media/Device Type

Type Of Media Or Device	Safeguards	Comments Or Additional Safeguards
Servers		
Desktops		
Home Computers		
Mobile Devices (Laptops, PDA, Phones, etc.)		
Shared Locations (Including drives and public folders)		
Email		
Applications		
Removable Media (CDs/DVDs, Diskettes/Tapes, Flash/Thumb Drives)		
Paper		
Internet		
Other (List)		

Appendix D: Reuse, Retirement and Destruction Form

Confidential

Date:

Department Name:

Information Owner/MPP:
Information Protection Form (Part 4 of 4)

Reuse, Retirement and Destruction

Type of Media or Device	Procedures	Frequency Of Destruction	Comments
Servers			
Desktops / Laptops			
Portable Devices (USB drives/Flash drives/PDAs)			
Writable CDs/DVDs			
Tapes/Diskettes			
Paper Copies			
Other (List)			

Appendix E: Data Classification Category Examples

Information Owners can use the following criteria to determine which data classification is appropriate for the respective institutional data or information system. A positive response to the highest category in any row is sufficient to place that data or system into that classification.

Category I (Confidential)

Confidential data is highly sensitive and may have personal privacy considerations, or may be protected restricted by, mandates, statutes, executive orders, policy and/or federal or state law and regulations (e.g., HIPPA, Sarbanes-Oxley, Gramm-Leach-Bliley).

Confidential Data (not all-inclusive) examples include:

- Passwords or credentials
- PINs (Personal Identification Numbers)
- Credit/debit/payment card numbers with any of the following:
    - Cardholder name
    - Expiration date
    - Card verification code
- Social Security number or Tax ID with name
- Birthdate with name and last four digits of social security number
- Driver's license number, state identification card, and other forms of international identification (such as passports, visas, etc.) with name or social security number
- Name with bank account information or bank account information with password, security code or any other access code information
- Private key (digital certificate)
- Health insurance information
- Medical records related to an individual (including disability information)
- Psychological counseling records related to an individual
- Electronic or digitized signatures
- Employee name with personally identifiable employee information:
    - Mother's maiden name
    - Race and ethnicity
    - Gender
    - Birthplace (city, state, country)
    - Employee net salary
    - Marital status
    - Physical description/personal characteristics
    - Employment history (including recruiting information)
    - Biometric information
    - Electronic or digitized signatures
    - Parents and other family member names

Category II (Restricted)

Restricted information must be guarded due to proprietary, ethical or privacy considerations. Restricted data is still subject to review or disclosure procedures to mitigate potential risks of inappropriate disclosure.

Restricted Data (not all-inclusive) examples include:

- Student name with personally identifiable educational records
  - Birth date (full: mm-dd-yyyy or partial: mm-dd only)
  - Courses taken
  - Schedule
  - Test scores
  - Financial aid received
  - Advising records
  - Educational services received
  - Disciplinary actions
  - Photograph
  - Most recent educational agency or institution attended
  - Participation in officially recognized activities and sports
  - Weight and height of members of athletic team
  - Grades
  - Fresno State identification number
  - Race & Ethnicity
  - Gender
  - Transcripts
  - Email addresses

- Employee name with personally identifiable employee information
  - Birth date (full: mm-dd-yyyy or mm-dd)
  - Emergency contact home address
  - Emergency contact personal telephone number
  - Emergency personal contact information (name, cell phone, pager)
  - Personal telephone numbers
  - Personal vehicle information
  - Personal email address
  - Parents and other family member names
  - Payment history
  - Employee evaluations
  - Background investigations

- Other
  - Legal investigations conducted by the Research Foundation
  - Sealed bids
  - Trade secrets or intellectual property such as research activities
  - Location of highly sensitive or critical assets (e.g. safes, check stocks, etc.)
  - Vulnerability or incident information
  - Licensed software
  - Attorney/client communications
  - Third party proprietary information per contractual

Category III (Unrestricted)

Unrestricted information is generally regarded as publicly available. This information is either explicitly defined as public information or not specifically classified as confidential or restricted information.

Unrestricted Data (not all-inclusive) examples include:

- Student information designated as Educational Directory Information (excluding grades):
  - Student name
  - Major field of study
  - Dates of attendance
  - Degrees, honors and awards received

- Employee Information (including student employment)
  - Employee title
  - Employee name (first, middle, last; except when associated with protected information)
  - Enrollment status
  - Department employed
  - Work location and telephone number
  - Work email address
  - Employee classification
  - Status as student (such as TA, GA, ISA)
  - Employee gross salary
  - Signature (non-electronic)