Information Protection Plan Workshop

Rafael Villegas, Ph.D.
Technical Information Security Officer
Technology Services
California State University, Fresno

08/18/2011

Outline

- Why Protect Confidential Information
- Confidentiality of Data Reporting Changes
- Information Protection Plan Summary
- Records and Retention Schedules
- Data Classification Examples
- Information Protection Forms
- Assistance

Why Protect Confidential Data

- **Federal and State Laws**
  - Information Practices Act of 1977
  - State Law SB1386 requires notification if there is a suspected incident involving unencrypted data with personal identifiers
  - FERPA
- **Health Insurance Portability and Accountability Act (HIPPA)**
  - First comprehensive Federal protection for the privacy of personal health information
- **CSU (Policies & Coded Memoranda)**
  - CSU Information Security Policy (CSU Administrative Manual)
  - HR 2005-16 (Requirements for Protecting Confidential Personal Information)
- **Fresno State Policies / Standards**
  - Data Classification Policy
  - Data Handling Standard
  - Protection of Confidential and Restricted Information (Memorandum)

Confidentiality Of Data Reporting Changes

- **1.0 Introduction**
  - 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

Information Protection Plan Summary

- **2.0 Policy Management**
  - The *Data Classification Policy* (approved in August 2009)
  - The *Data Handling Standard* (approved in February 2010)
  - Policies located at
    - http://www.csufresno.edu/technology/policies/index.shtml

- **3.0 Asset Management**
  - A designated information (data) owner for each respective type of data
    - "Custodian of Records" is the designated Information (Data) Owner, identified at http://www.csufresno.edu/adminserv/records/
    - Otherwise highest ranking MPP of respective area is the designated Information (Data) Owner
  - Inventory confidential and restricted data and information resources
  - Data retention/disposal in accordance with CSU executive order 1031
  - Three categories of data classification
    - Confidential
    - Restricted
    - Unrestricted

Information Protection Plan Summary

- **4.0 Human Resources Management**
  - Only necessary information is collected.
  - Roles and responsibilities
  - 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**
  - Confidential and restricted documents are filed with appropriate file covers and/or markings identifying their classification category
  - The university has a clear desk and clear screen requirement for areas that handle confidential or restricted data
  - 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
  - Electronic media and information resources are sanitized and/or destroyed appropriately

Information Protection Plan Summary

- **6.0 Communication and Operations Management**
  - Software is not downloaded and installed on information resources without appropriate authorization
  - Backup and recovery procedures are documented, tested and available
  - Transmission (verbal, facsimile, telephone, electronic) of confidential and restricted data requirements

- **7.0 Access Management**
  - User access requirements
    - Best practices for password protection
    - MPP authorizes user access
    - User access is periodically reviewed
  - Audit logging process is implemented to maintain the confidentiality and integrity of data and information resources

Information Protection Plan Summary

- **8.0 Systems Acquisition, Development and Maintenance**
  - Operational software is to be maintained at a level supported by the vendor and to the latest patch level possible
  - All confidential and restricted data is encrypted, using a university approved encryption solution, on:
    - Removable media
    - Non-university owned devices
    - All portable (mobile) device able to comply
    - All workstations (i.e. computers)
    - Servers not located in a dedicated server room with physical access controls

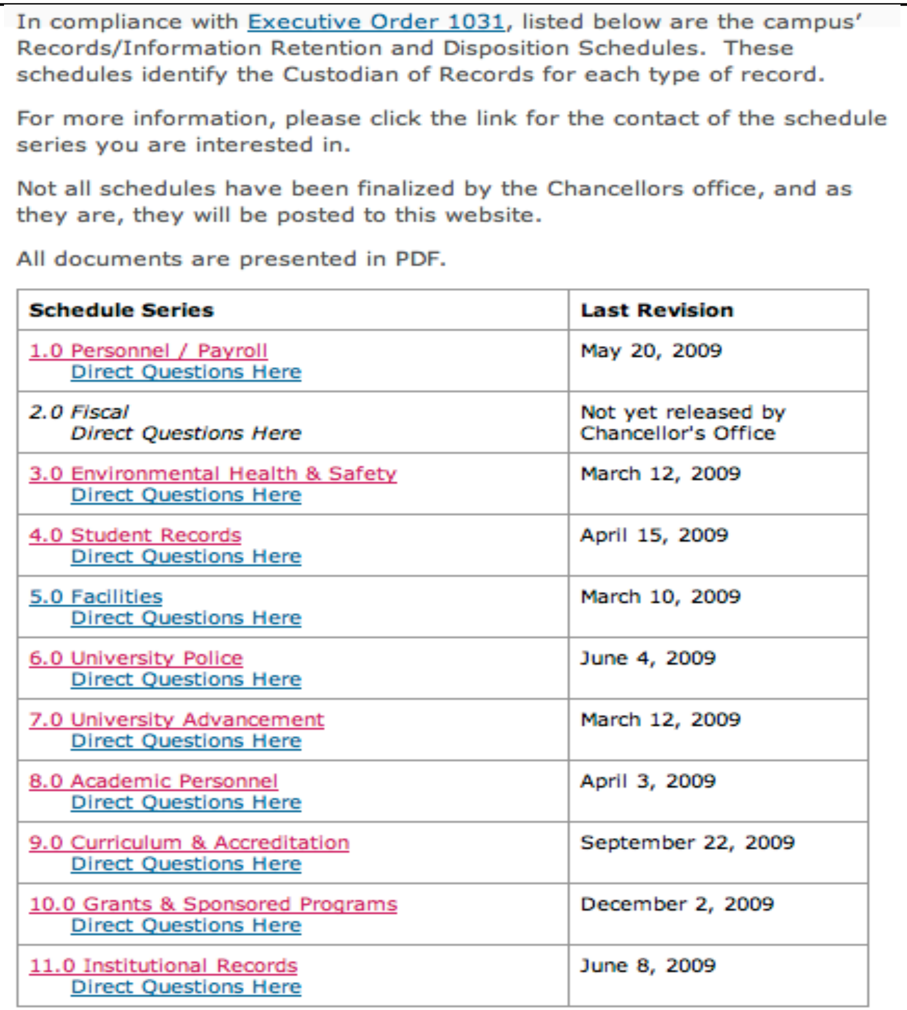
- **9.0 Incident Management**
  - All information security incidents are promptly reported

Information Protection Plan Summary

- **10.0 Business Continuity Management**
  - Business continuity plans are reviewed and tested
  - Disaster recovery plans ensure the availability of data and servers can be restored following a disaster

- **11.0 Compliance Management**
  - Complete the forms that can be downloaded from the Help Desk at https://help.csufresno.edu under the staff and faculty forms section
    - Self assessment form
    - Inventory form
    - Media type form
    - Reuse, retirements and destruction form

Records Retention and Disposition (http://www.csufresno.edu/adminserv/records/)



In compliance with Executive Order 1031, listed below are the campus' Records/Information Retention and Disposition Schedules. These schedules identify the Custodian of Records for each type of record.

For more information, please click the link for the contact of the schedule series you are interested in.

Not all schedules have been finalized by the Chancellors office, and as they are, they will be posted to this website.

All documents are presented in PDF.

Schedule Series	**Last Revision**
1.0 Personnel / Payroll Direct Questions Here	May 20, 2009
2.0 Fiscal *Direct Questions Here*	Not yet released by Chancellor's Office
3.0 Environmental Health & Safety Direct Questions Here	March 12, 2009
4.0 Student Records Direct Questions Here	April 15, 2009
5.0 Facilities Direct Questions Here	March 10, 2009
6.0 University Police Direct Questions Here	June 4, 2009
7.0 University Advancement Direct Questions Here	March 12, 2009
8.0 Academic Personnel Direct Questions Here	April 3, 2009
9.0 Curriculum & Accreditation Direct Questions Here	September 22, 2009
10.0 Grants & Sponsored Programs Direct Questions Here	December 2, 2009
11.0 Institutional Records Direct Questions Here	June 8, 2009

Data Classification Examples

- **Category I (Confidential) – Examples (not all-inclusive)**
- 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
- Health insurance information
- Medical records related to an individual (including disability information)
- Psychological counseling records related to an individual
- Employee name with personally identifiable employee information:
  - Mother’s maiden name
  - Race and ethnicity
  - . . .
- **. . .**

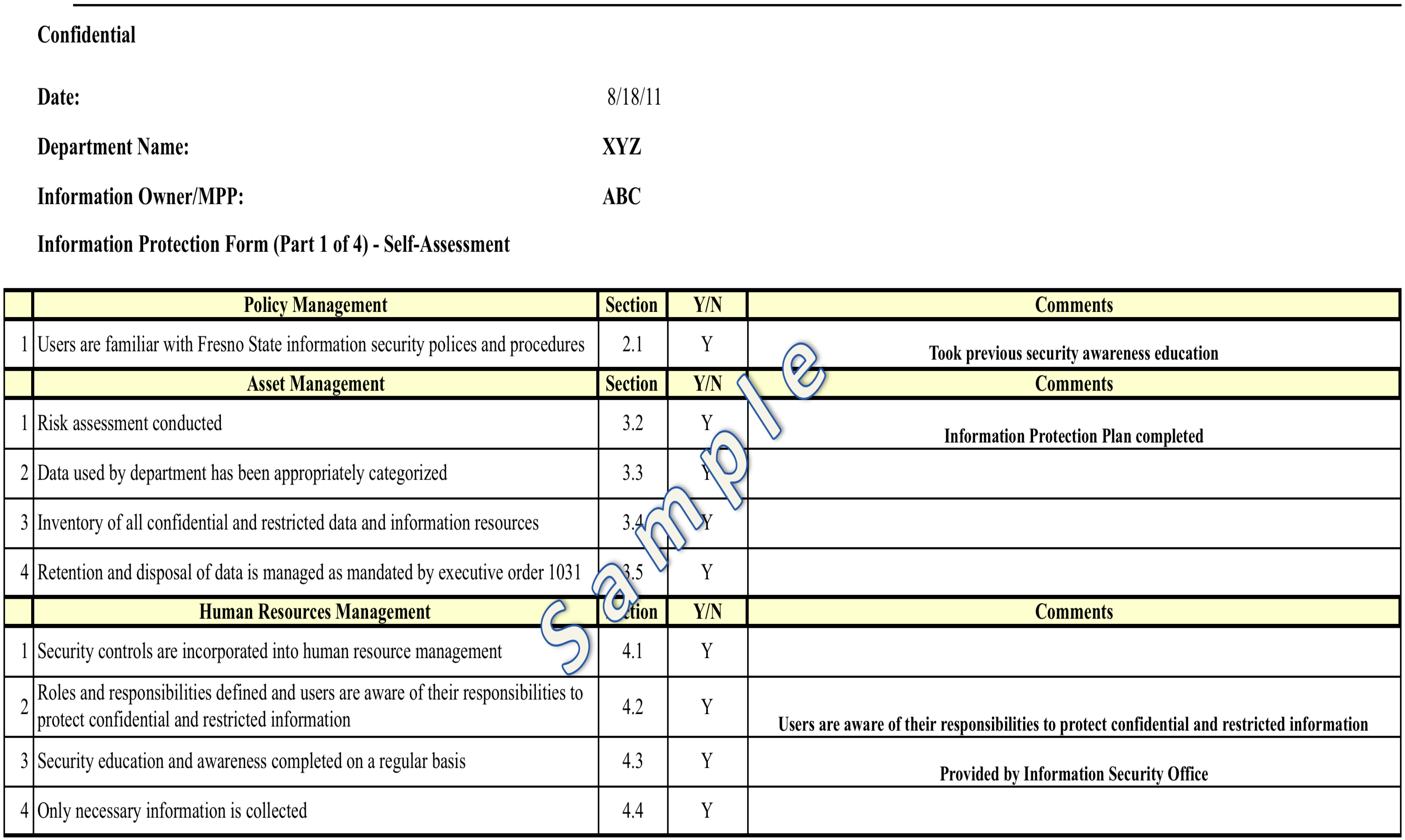
Data Classification Examples

- **Category II (Restricted) – Examples (not all-inclusive)**
- Student name with personally identifiable educational records
  - Birth date (full: mm-dd-yyyy or partial: mm-dd only)
  - Courses taken
  - Test scores
  - Financial aid received
  - Advising records
  - . . .
- 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
  - . . .
- Other
  - Legal investigations conducted by the Research Foundation
  - Trade secrets or intellectual property such as research activities
  - Location of highly sensitive or critical assets (e.g. safes, check stocks, etc.)
  - . . .

Data Classification Examples

- **Category III (Unrestricted) – Examples (not all-inclusive)**
- 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
  - . . .

Self-Assessment Form (continued)



Confidential

Date: 8/18/11

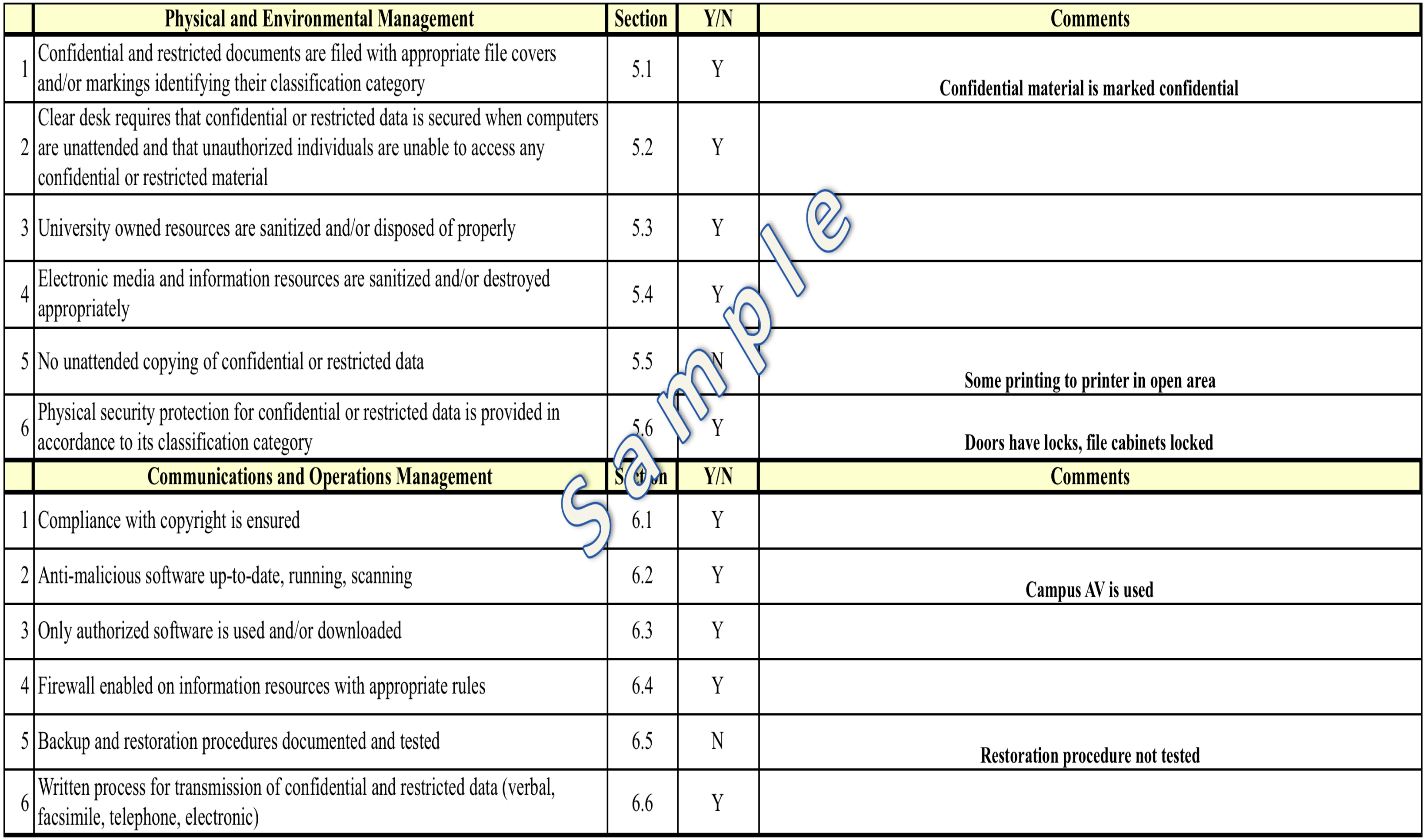
Department Name: **XYZ**

Information Owner/MPP: **ABC**

Information Protection Form (Part 1 of 4) - Self-Assessment

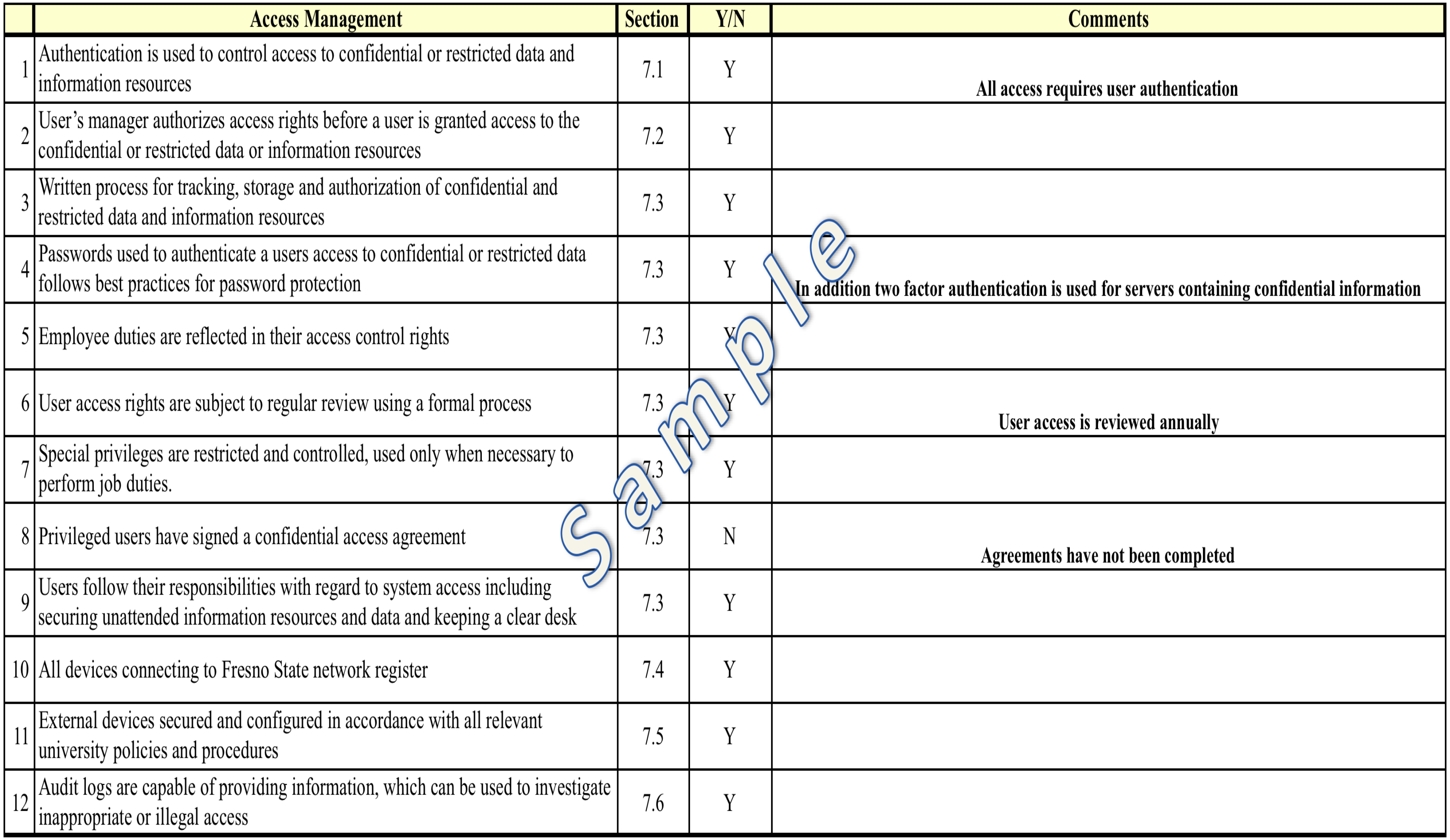
	Policy Management	**Section**	**Y/N**	**Comments**
1	Users are familiar with Fresno State information security polices and procedures	2.1	Y	**Took previous security awareness education**
	Asset Management	**Section**	**Y/N**	**Comments**
1	Risk assessment conducted	3.2	Y	**Information Protection Plan completed**
2	Data used by department has been appropriately categorized	3.3	Y	
3	Inventory of all confidential and restricted data and information resources	3.4	Y	
4	Retention and disposal of data is managed as mandated by executive order 1031	3.5	Y	
	Human Resources Management	**Section**	**Y/N**	**Comments**
1	Security controls are incorporated into human resource management	4.1	Y	
2	Roles and responsibilities defined and users are aware of their responsibilities to protect confidential and restricted information	4.2	Y	**Users are aware of their responsibilities to protect confidential and restricted information**
3	Security education and awareness completed on a regular basis	4.3	Y	**Provided by Information Security Office**
4	Only necessary information is collected	4.4	Y	

Self-Assessment Form (continued)



	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	Y	**Confidential material is marked confidential**
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	Y	
3	University owned resources are sanitized and/or disposed of properly	5.3	Y	
4	Electronic media and information resources are sanitized and/or destroyed appropriately	5.4	Y	
5	No unattended copying of confidential or restricted data	5.5	N	**Some printing to printer in open area**
6	Physical security protection for confidential or restricted data is provided in accordance to its classification category	5.6	Y	**Doors have locks, file cabinets locked**
	Communications and Operations Management	**Section**	**Y/N**	**Comments**
1	Compliance with copyright is ensured	6.1	Y	
2	Anti-malicious software up-to-date, running, scanning	6.2	Y	**Campus AV is used**
3	Only authorized software is used and/or downloaded	6.3	Y	
4	Firewall enabled on information resources with appropriate rules	6.4	Y	
5	Backup and restoration procedures documented and tested	6.5	N	**Restoration procedure not tested**
6	Written process for transmission of confidential and restricted data (verbal, facsimile, telephone, electronic)	6.6	Y	

Self-Assessment Form (continued)



	Access Management	Section	Y/N	Comments
1	Authentication is used to control access to confidential or restricted data and information resources	7.1	Y	All access requires user authentication
2	User's manager authorizes access rights before a user is granted access to the confidential or restricted data or information resources	7.2	Y	
3	Written process for tracking, storage and authorization of confidential and restricted data and information resources	7.3	Y	
4	Passwords used to authenticate a users access to confidential or restricted data follows best practices for password protection	7.3	Y	In addition two factor authentication is used for servers containing confidential information
5	Employee duties are reflected in their access control rights	7.3	Y	
6	User access rights are subject to regular review using a formal process	7.3	Y	User access is reviewed annually
7	Special privileges are restricted and controlled, used only when necessary to perform job duties.	7.3	Y	
8	Privileged users have signed a confidential access agreement	7.3	N	Agreements have not been completed
9	Users follow their responsibilities with regard to system access including securing unattended information resources and data and keeping a clear desk	7.3	Y	
10	All devices connecting to Fresno State network register	7.4	Y	
11	External devices secured and configured in accordance with all relevant university policies and procedures	7.5	Y	
12	Audit logs are capable of providing information, which can be used to investigate inappropriate or illegal access	7.6	Y	

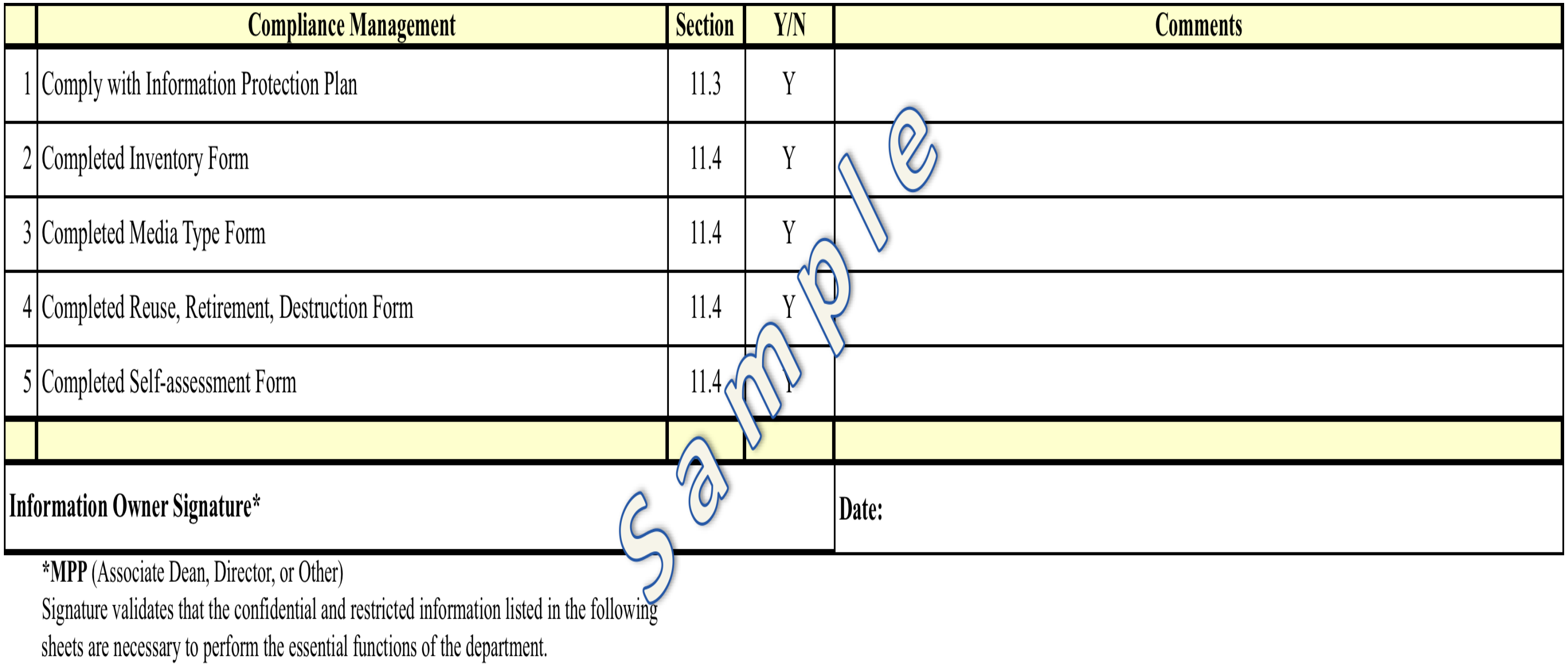
Self-Assessment Form (continued)

	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	Y	
2	Operational software is maintained at a level supported by the vendor and to the latest patch level possible	8.2	Y	
3	Appropriate encryption key lengths and key strengths are used based on the classification of the data or information resource	8.3	Y	
4	All confidential and restricted data is encrypted on servers not in a secure dedicated server room	8.3.1	Y	
5	All confidential and restricted data stored on workstations (i.e. computers) is encrypted	8.3.2	Y	
6	All mobile devices that process and/or store confidential or restricted data are encrypted	8.3.3	N	
7	All confidential and restricted data on removable media is encrypted	8.3.4	N	**Confidential data on DVD is not encrypted**
8	All confidential and restricted data on non-university owned information resources is encrypted	8.3.5	N	**Some non-university owned resources are not encrypted**
9	Vulnerability assessments conducted on information resources containing confidential or restricted information	8.4	Y	**Vulnerability scans conducted before resource placed in production**

	Incident Management	Section	Y/N	Comments
1	Incidents promptly reported	9.1	Y	
2	Written incident reporting procedures	9.2	Y	

	Business Continuity Management	Section	Y/N	Comments
1	Developed business continuity plans	10.1	N	**Plans not completed**
2	Developed disaster recovery plans	10.2	N	

Self-Assessment Form (continued)

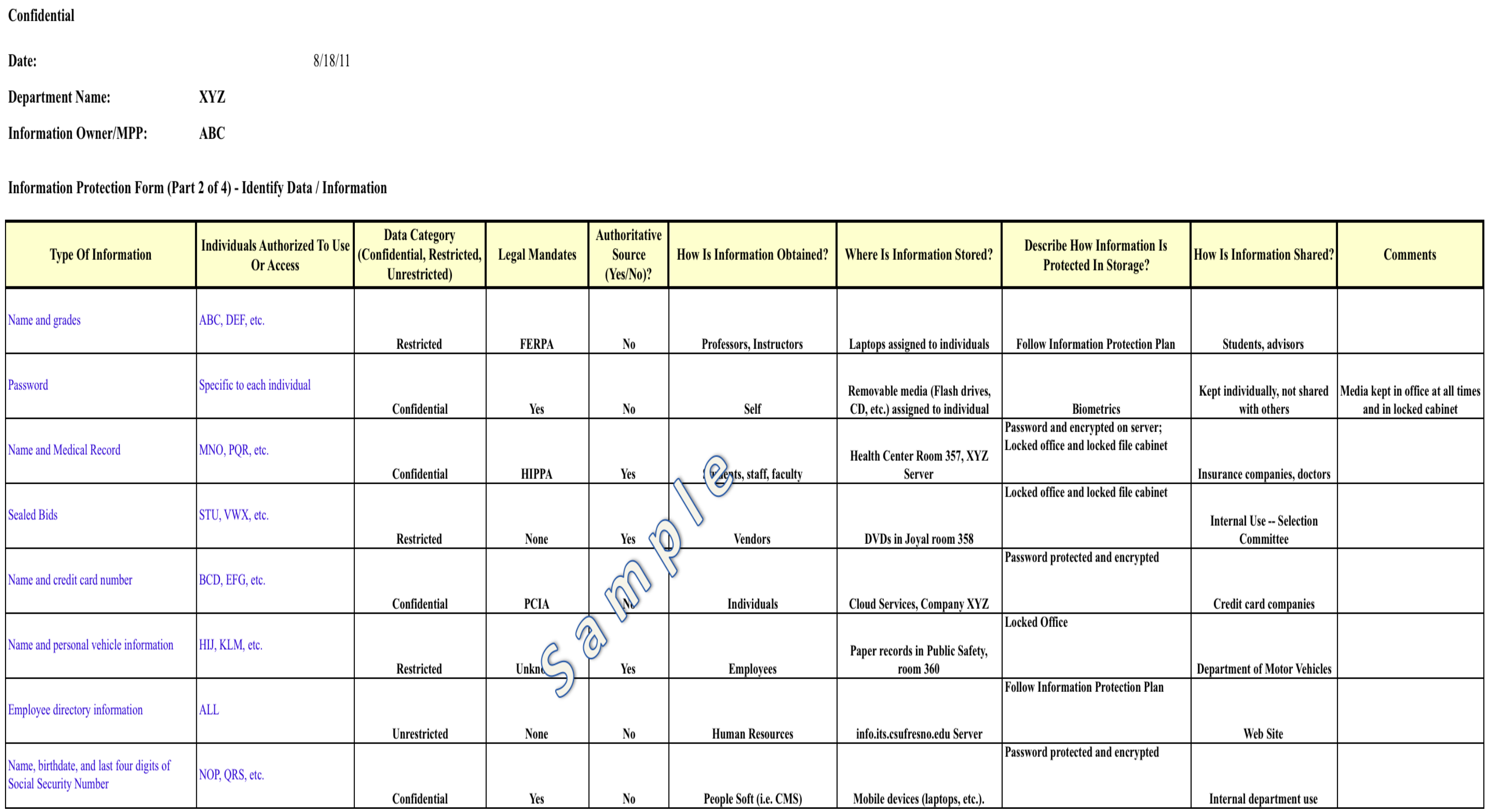


	Compliance Management	Section	Y/N	Comments
1	Comply with Information Protection Plan	11.3	Y	
2	Completed Inventory Form	11.4	Y	
3	Completed Media Type Form	11.4	Y	
4	Completed Reuse, Retirement, Destruction Form	11.4	Y	
5	Completed Self-assessment Form	11.4	Y	

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.

Inventory Form



Confidential

Date: 8/18/11

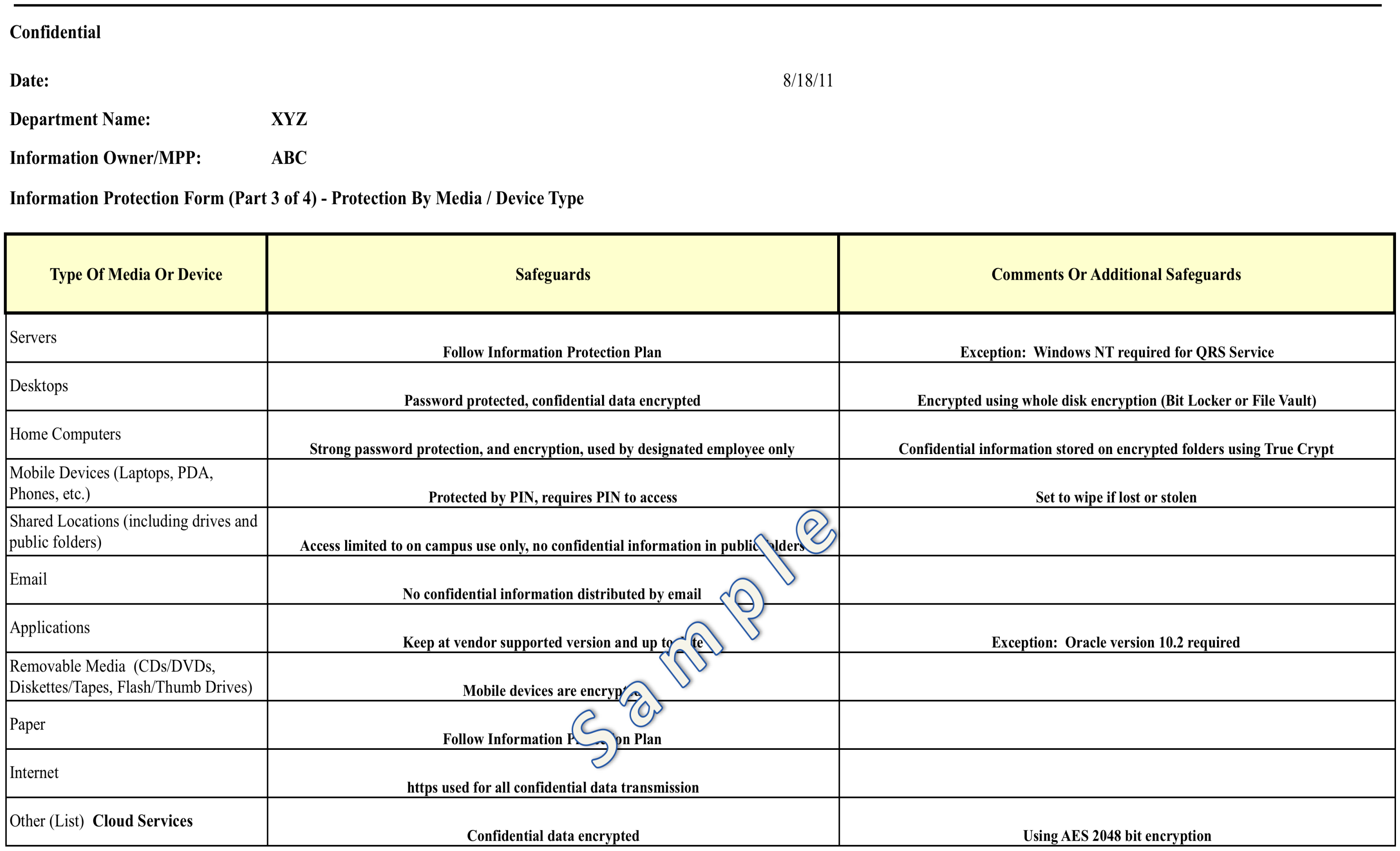
Department Name: XYZ

Information Owner/MPP: ABC

Information Protection Form (Part 2 of 4) - Identify Data / Information

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
Name and grades	ABC, DEF, etc.	Restricted	FERPA	No	Professors, Instructors	Laptops assigned to individuals	Follow Information Protection Plan	Students, advisors	
Password	Specific to each individual	Confidential	Yes	No	Self	Removable media (Flash drives, CD, etc.) assigned to individual	Biometrics	Kept individually, not shared with others	Media kept in office at all times and in locked cabinet
Name and Medical Record	MNO, PQR, etc.	Confidential	HIPPA	Yes	Students, staff, faculty	Health Center Room 357, XYZ Server	Password and encrypted on server; Locked office and locked file cabinet	Insurance companies, doctors	
Sealed Bids	STU, VWX, etc.	Restricted	None	Yes	Vendors	DVDs in Joyal room 358	Locked office and locked file cabinet	Internal Use -- Selection Committee	
Name and credit card number	BCD, EFG, etc.	Confidential	PCIA	No	Individuals	Cloud Services, Company XYZ	Password protected and encrypted	Credit card companies	
Name and personal vehicle information	HIJ, KLM, etc.	Restricted	Unknown	Yes	Employees	Paper records in Public Safety, room 360	Locked Office	Department of Motor Vehicles	
Employee directory information	ALL	Unrestricted	None	No	Human Resources	info.its.csufresno.edu Server	Follow Information Protection Plan	Web Site	
Name, birthdate, and last four digits of Social Security Number	NOP, QRS, etc.	Confidential	Yes	No	People Soft (i.e. CMS)	Mobile devices (laptops, etc.).	Password protected and encrypted	Internal department use	

Media Type Form



Confidential

Date: 8/18/11

Department Name: **XYZ**

Information Owner/MPP: **ABC**

Information Protection Form (Part 3 of 4) - Protection By Media / Device Type

Type Of Media Or Device	Safeguards	Comments Or Additional Safeguards
Servers	**Follow Information Protection Plan**	**Exception: Windows NT required for QRS Service**
Desktops	**Password protected, confidential data encrypted**	**Encrypted using whole disk encryption (Bit Locker or File Vault)**
Home Computers	**Strong password protection, and encryption, used by designated employee only**	**Confidential information stored on encrypted folders using True Crypt**
Mobile Devices (Laptops, PDA, Phones, etc.)	**Protected by PIN, requires PIN to access**	**Set to wipe if lost or stolen**
Shared Locations (including drives and public folders)	**Access limited to on campus use only, no confidential information in public folders**	
Email	**No confidential information distributed by email**	
Applications	**Keep at vendor supported version and up to date**	**Exception: Oracle version 10.2 required**
Removable Media (CDs/DVDs, Diskettes/Tapes, Flash/Thumb Drives)	**Mobile devices are encrypted**	
Paper	**Follow Information Protection Plan**	
Internet	**https used for all confidential data transmission**	
Other (List) **Cloud Services**	**Confidential data encrypted**	**Using AES 2048 bit encryption**

Reuse, Retirements, and Destruction Form

Confidential

Date: 8/18/11

Department Name: **XYZ**

Information Owner/MPP: **ABC**

Information Protection Form (Part 4 of 4) - Reuse, Retirement and Destruction

Type of Media or Device	Procedures	Frequency Of Destruction	Comments
Servers	**Disk drives removed and physically destroyed (shredded)**	**Refresh cycle (every three years)**	
Desktops / Laptops	**Disk drives wiped**	**During refresh and re-allocation of systems**	**7 pass - DOD approved wipe for internal re-use** **35 pass - DOD approved wipe for surplus**
Portable Devices (USB drives/Flash drives/PDAs)	**Erased using 7-pass wipe**	**Monthly**	
Writable CDs/DVDs	**Shredded**	**As required**	
Tapes/Diskettes	**De-gauzed**	**Follow retention and disposition schedule**	
Paper Copies	**Shredded using cross-cut shredder**	**Follow retention and disposition schedule**	
Other (List) **IPhone**	**Data erased**	**As needed**	**Set to wipe if lost or stolen**

Assistance

- **Information Security Office**
  - Rafael Villegas, Ph.D.
    - Email: rafael@csufresno.edu
    - Phone: 278-7941
  - Jim Michael
    - Email: jimm@csufresno.edu
    - Phone: 278-7001
- **IT Liaisons**
  - Assistance with encryption
  - Assistance in completing forms
    - Media Type Form (part 3)
    - Reuse, Retirement and Destruction Form (part 4)
    - Inventory Form (part 2)
- **Help Desk**
  - Downloading Information Protection Plan and Forms