Changes To Confidentiality Of Data Reporting

1.0 Introduction

There have been a number of changes, since plans for protection of confidentiality of data were updated in 2008, which Chairs and department managers need to take into consideration as they prepare to update their Information Protection Plans.

These changes include new university policies and standards, new requirements stated in Executive Orders from the Chancellor and updated procedures intended to establish common practices for protecting confidential and restricted data and reduce the work required to keep Information Protection Plans current.

A university Information Protection Plan is being adopted to facilitate the update and maintenance of these plans. Procedures are being implemented to allow department managers to certify compliance with University, Division and College/School plans and to refer to these plans in their departments' Information Protection Plans.

The intent of these plans and procedures is to allow departments' plans to focus on the inventory of their confidential and restricted data and any department-specific requirements or practices without having to restate practices defined in higher-level plans that are followed in the department.

Information Security has also developed a self-assessment and templates for the inventory and other information required in the departmental plans. These documents should simplify the process of updating and maintaining these plans and certifying compliance with the university Information Protection Plan.

The items below outline the new policy changes and the key practices included in the Information Protection Plan being developed for the University:

2.0 Policy Management

- Data Classification Policy - our campus approved a new data classification policy in August 2009 that defines how the university will classify data in order to apply appropriate level of resources to the protection of institutional data based upon requirements.
- Data Handling Standard – our campus adopted a new data handling standard in February 2010 that defines an information owner based on Executive Order 1031 and facilitates the identification, management and requirements for the protection of university data.

These policies are located at http://www.csufresno.edu/technology/policies/index.shtml.

3.0 Asset Management

- A designated information (data) owner is now required for each respective type of data.
- Three categories of classification are defined to maintain appropriate protection of university data:
    - Category I (Confidential Data)
    - Category II (Restricted Data)
    - Category III (Unrestricted Data)

- University policy and standards now require an information protection plan from each department which includes:
    - An inventory of all confidential and restricted data and information resources.
    - A description on how this data is protected in any form (paper or electronic) or media.
    - An account on how the retention and disposal of data is managed in accordance with CSU executive order 1031.

4.0 Human Resources Management

- 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.
- Security education and awareness program provided on a regular basis.
- Only necessary information is collected.

5.0 Physical and Environmental Management

- Confidential and restricted documents are filed with appropriate file covers and/or markings identifying their classification category.
- Clear desk procedures, at close of business:
    - Ensure that no confidential or restricted information is left unsecured.
    - Quit all systems and networks and where possible shut down their computers.
    - University owned resources are sanitized and/or disposed of properly.
- 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.

6.0 Communications and Operations Management

- Firewalls implementation on servers, computers and network-connected devices.
- Backup frequency is based on business risks and backup restoration procedures are documented.
- Transmission (verbal, facsimile, telephone, electronic) of confidential and restricted data requirements.

7.0 Access Management

- Passwords used to authenticate a user's access to confidential or restricted data follow best practices for password protection.
- All devices connecting to the Fresno State Network register.
- An audit logging process is implemented to maintain the confidentiality and integrity of data and information resources.

8.0 Systems Acquisition, Development and Maintenance

- Operational software is 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 workstation (i.e. computers).
  - All servers not located in a dedicated server room with physical access controls.

9.0 Incident Management

- All information security incidents are promptly reported.
- Loss or theft of university resources is reported to the University Police Department.

10.0 Business Continuity Management

- Business continuity plans are reviewed and tested.
- Disaster recovery plans ensure the availability of data and services can be restored following a disaster.

11.0 Compliance Management

Confirmation of the *Information Protection Plan* requires completion of the following forms:

- Self-assessment form (i.e. conformance with *Information Protection Plan*)
- Inventory form (i.e. authorized use and access, location, and distribution)
- Media type form (i.e. identification of information resources and safeguards)
- Reuse, retirements and destruction (i.e. proper disposal of data and resources)

These forms, including the information protection workshop presentation, can be downloaded from the Help Center web site.

To view or download these documents, please go to the staff and faculty forms section at https://help.csufresno.edu/forms/index.php?userclass=facstaff and log in with your campus userid and password. After login in, scroll down to the section entitled "Information (Data) Protection Documents" to obtain the documents.