



Information Security Risk Assessment

Cal State L.A. required to perform an annual review and report.

In this Issue

- 1. Information Security Risk Assessment**
- 1. FERPA Recertification**
- 2. Identity Finder – At a Glance**
- 3. Annual Calendar of Information Security Responsibilities**
- 3. User Guidelines for Mobile Computing**
- 4. User Access Controls for Decentralized Systems**
- 4. Administrative Systems' Access Modification Forms**

The CSU Information Security Policy, section 8020.0, requires all campuses to develop risk management processes that identify, assess and monitor risks to information assets containing [Levels 1 and 2](#) data.

The vice presidents have overall responsibility for assigning risk assessment, ensuring mitigation occurs and approving risk acceptance within their respective divisions. Once risks are identified, the campus can develop and implement strategies to reduce the risk to acceptable levels, shift the risk to another party or assume the identified risk.

To begin the identification process, there is an online [Information Security Risk Assessment Worksheet](#) that all employees can use to record information about their work areas. The worksheet, which addresses physical security, electronic documents and paper documents, is brief, primarily involves checking boxes and can be completed in about ten minutes. The information provided on the worksheet also references the use of [Identity Finder](#), the desktop tool already available on desktops that can identify and protect sensitive data. (Check out page 2 to view our Identity Finder progress.)

Information from the worksheet is collected electronically and a consolidated report is prepared and submitted annually to the vice president of each division for their review and action.

FERPA Recertification

Every employee with network access, an e-mail account or administrative system access must complete a FERPA recertification review EVERY TWO YEARS. Your *myCSULA Identity* account automatically verifies your last FERPA date and sends an e-mail reminder to take the refresher tutorial and brief test, and submit the printed certificate to HRM for filing in your official personnel file.

Start the [FERPA Tutorial](#) now!

2012 Risk Assessment Deadlines

- | | |
|------------------|--|
| July 13 | Last date for employees to complete the online worksheet. |
| July 16 | Data extraction and report preparation begins. |
| July 23 | Report distributed to the vice presidents. |
| August 15 | Vice presidents' Risk Remediation/Acceptance report due to the University internal auditor. |





AT A GLANCE

Just how much unencrypted sensitive information has the campus identified and secured or safely destroyed? Take a look below at our progress. As you can see, we still have much work to do, but these statistics indicate we are beginning progress toward securing 100% of the sensitive data on our campus computers.

If you have cleaned your computer, keep up the good work! Remember to always [encrypt documents](#) with sensitive information as you create or modify them. If you haven't yet run [Identity Finder](#), just click on the blue dog icon on your desktop or if you cannot locate the icon, contact the ITS Help Desk at 3-6170 for assistance. Identity Finder runs in the background so you can continue your work without interruption. Once the files have been identified, you can return later to secure or destroy them.

Type of Data	Data Matches As of December 2, 2011	Data Matches As April 12, 2012
Number of computers scanned	248	333
Potential Social Security numbers and CINs	6,050,903	8,743,164
E-mail addresses	149,499	159,436
Credit card numbers	45,092	94,792
Passwords	42,851	45,100
Personal addresses	36,092	250,509
Telephone numbers	24,894	314,651
Bank account numbers	5,247	18,912
Dates of birth	3,223	7,394
Driver's license numbers	5	6

Overall progress toward securing 100% of data on campus computers

333	1915*
------------	--------------

* Denotes quantity of Identity Finder apps currently deployed

Calendar of Upcoming Information Security Responsibilities

Over the last decade, legislation covering information security has increased, security standards have tightened and audits have become more frequent and detailed. To meet these challenges, ITS routinely issues standards and guidelines to inform employees of their [roles and responsibilities](#) toward protecting our information assets. The CSU Board of Trustees' auditors are now requiring that our campus submit documentation to support our claims that we are meeting security standards and that all employees are completing the responsibilities delegated to them. To ensure we can achieve that requirement, here is a reminder of upcoming tasks and reports that may require your attention.

Deadline	Responsible Entity	Action Required
Monthly	Identity Theft Prevention Program department administrators	Submit the monthly log of identity theft events, if any, to the director, IT Security and Compliance.
Monthly	Department administrators	Review and remove any approved third-party system access rights that are no longer required. Retain remediation documentation, if any.
Monthly	Department administrators	Survey work areas to ensure printed documents with Levels 1 and 2 data are not exposed.
April 20	Department administrators with decentralized systems	Submit quarterly User Access Control report to the internal auditor.
June 30	All system data stewards	Review, verify and revise as necessary user access rights to campus information assets. Look for employees who have changed positions and remove or update access accordingly. Retain documentation.
June 30	All MPPs	Update and review the annual inventory of mobile devices authorized by the department to contain protected data. Retain documentation.
July 13	Department administrators with decentralized systems	Submit quarterly User Access Control report to the internal auditor.
July 13	All employees	Deadline to complete the online Risk Assessment Worksheet .
July 23	Director, IT Security and Compliance	Deliver annual Risk Assessment report to the vice presidents.
August 15	All vice presidents	Deliver annual Risk Acceptance/Remediation Report to the internal auditor.

User Guidelines for Mobile Computing

In February 2012, ITS issued a new information security guideline - [ITS-1020-G User Guidelines for Mobile Computing](#).

This guideline establishes an authorized method for controlling mobile computing devices that contain or access CSULA protected data. The guidelines are designed to preserve the integrity, availability and confidentiality of this data, and apply to both institutional and privately owned/funded devices.

Mobile computing devices include any portable device such as a laptop, tablet PC, Personal Digital Assistant (PDA), cell phone or smart phone that is capable of storing, processing, displaying and communicating data and is equipped with wireless or wired communications capability.

If you use any of these devices for University business, please take the time to read this important guideline. It will provide you valuable information to set up physical security, prevent unauthorized access and travel safely with your device both domestically and internationally.

User Access Controls for Decentralized Systems

The CSU Board of Trustees' auditors require departmental decentralized systems to meet the same user access controls as those administrative systems managed centrally by Information Technology Services.

What is a decentralized system?

A decentralized system is defined as “*any data system or equipment containing data deemed private or confidential or which contains mission critical data, including departmental, divisional or other ancillary system or equipment that is not managed by central ITS.*”

What are these required access controls?

There are three levels of controls– Department Access Controls, System Administrator Access Controls and User Access Controls.

What are the Department Access Controls?

Departments are required to establish and document formal procedures for each decentralized system that minimally provides for the following: physical security, a formal user access request procedure and form, defined user roles, review and approval of the user access request prior to access being granted, access removal for any employee no longer requiring access and immediate removal of terminated employees' access.

What are the System Administrator Access Controls?

System administrators (sys admins) cannot review or approve access forms, each sys admin must have a unique user id that defines the individual, each user must have a unique user ID that matches his or her domain user id, sys admins cannot share their access rights, and systems, data and backups must be physically and logically secured.

What are the User Access Controls?

Users must: apply for access to decentralized systems, have a signed access and compliance form on file with Human Resources Management, have a valid FERPA certificate on file with HRM, meet all University password standards and not share or log other individuals onto the decentralized system.

Are there any oversight requirements?

Yes. A quarterly report must be prepared for every decentralized system and submitted to the University internal auditor by the third week of each quarter.

System data stewards or system administrators are responsible for preparing the quarterly report of system user access.

Department administrators are responsible for reviewing, approving and submitting the final report to the internal auditor. They are also responsible for ensuring remediation of any identified non-compliance issues.

More information on this topic, including detailed quarterly report components and designated responsibilities, is available in [*ITS-2011-S User Access Control for Decentralized Systems*](#).

Access Modification Forms for Administrative Systems

Important Reminder...

When an employee moves from a department, or takes another position as a result of a promotion or other type of transfer, please remember to complete the relevant system modification form to address the change in access. ITS user forms are available online at:

<http://www.calstatela.edu/its/forms>

Without the modification form, previous employees will continue to have access to your department's information assets.