## User Guidelines for Access to Administrative Information Systems

| | | | |
|---|---|---|---|
| Guideline No. | ITS-1014-G | Rev: | D |
| Owner: | IT Security and Compliance | | |
| Approved by: | Sheryl Okuno, Director<br>IT Security and Compliance | | |
| Issued: | 2/24/06 | Revised: | 4/24/13 |

## Table of Contents

## 1 Purpose

The University's administrative information systems provide mission-critical functions that users access on a daily basis. The University recognizes administrative information systems as a University resource requiring proper management in order to permit effective planning and decision-making and to conduct business in a timely and productive manner.  Administrative information systems provide abundant opportunities for easy and efficient access to data but also pose significant risk to the security of administrative information since these systems generally store protected data.  Therefore, access to these systems must be strictly controlled and limited to only authorized personnel.

The purpose of this guideline is to ensure that administrative information system users experience uninterrupted access to administrative data and systems, can trust the integrity of administrative data and systems, and are confident that protected data is treated with care.

## 2 Entities Affected by Guidelines

This guideline pertains to all University administrative information systems and the users of those systems.

## 3 Definitions

a. Administrative Information:  Any data related to the business of the University including, but not limited to, financial, human resources, students and contributor relations.  It includes data maintained at the departmental and office level as well as centrally, regardless of the media on which the data resides.

b. Administrative Information Systems:  Any University information system that supports the storage, retrieval and maintenance of information supporting a major administrative function of the University and any associated administrative data that resides on end-users' local desktop computers and/or departmental servers. Administrative information systems do not include systems that directly support the teaching and learning and research activities of the University.

c. Anti-virus Software: Programs to detect and remove computer viruses.  The simplest anti-virus programs scan executable files and boot blocks for a list of known viruses.  Others are constantly active, attempting to detect the actions of general classes of viruses.  Anti-virus software should always include a regular update service that downloads the latest virus definitions and "inoculations."

d. Common Financial System (CFS): A CSU administrative system that consolidates campus financial information into a centralized database available to users with a job-related need to access this data.

e. Common Management System (CMS): A CSU-wide program initiated in 1998 that centralized Human Resources (HR), Student Administration (SA) and Financials (CFS) administrative systems throughout the CSU campuses and designated management of system resources to a central administrative location.

f. Confidential Information: See Level 1 Confidential Data and Level 2 Internal Use Data. Confidential information must be interpreted in combination with all information contained on the computer or electronic storage device to determine whether a violation has occurred.

g. Contributor Relations System (CR): A campus-based administrative system that consolidates information about campus contributors into a database available to users with a job-related need to access this data.

h. Human Capital Management System (HCM): A CSU administrative system that consolidates campus information for Student Administration (SA) and Human Resources (HR) into a centralized database available to users with a job-related need to access this data.

i. Level 1 Confidential Data: Confidential data 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. Its unauthorized use, access, disclosure, acquisition, modification, loss or deletion could result in severe damage to the CSU, its students, employees or customers. Financial loss, damage to the CSU's reputation and legal action could occur if data is lost, stolen, unlawfully shared or otherwise compromised. Level 1 data 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 data to persons outside of the University is governed by specific standards and controls designed to protect the information.

j. Level 2 Internal Use Data: Internal use data is information that 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, violate an individual's privacy rights or make legal action necessary. Non-directory educational information may not be released except under certain prescribed conditions.

k. Personal Information: California Civil Code 1798.29 defines personal information as: An individual's first name or first initial and last name in combination with any one or more of the following data elements:

- Social Security number
- Driver's license or California Identification Card number
- Account number, or credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account
- Medical information
- Health insurance information

l. Protected Data: An all-encompassing term that includes any information defined herein as confidential, personal, proprietary, health insurance, or medical information. See Level 1 Confidential Data and Level 2 Internal Use Data.

m. Security Administrator: Individual(s) who are responsible for security aspects of a system on a day-to-day basis.

n. System Administrator: Individual(s) who manage, operate, support campus information systems or manage networks. Duties generally include installation, support of operating system and application software, security, troubleshooting and training.

o. Third-party Service Providers: Refers to an entity that is undertaking an outsourced activity on behalf of the University or is performing system administrator duties on their offsite system that contains University protected data (e.g., vendors, vendor's subcontractors, business partners, consultants, etc.).

p. User: Users are one or more of the following:
   - Anyone or any system that accesses CSULA information assets.
   - Individuals who need and use University data as part of their assigned duties or in fulfillment of assigned roles or functions within the University community.
   - Individuals who are given access to sensitive data, have a position of special trust and as such are responsible for protecting the security and integrity of those data.

# 4 Guidelines

CSULA administrative information systems are for employees and third-party service providers whose use is based on written authorization. Limited access is also granted to employees and students for the purpose of viewing and maintaining self-service applications.

## 4.1 User Responsibilities

University administrative information systems and data are for use only by the individual granted access.

Users must:

- Only use administrative information systems for the sole purpose of conducting official University business.
- Access administrative information systems based on their need to use specific data, as defined by job duties, and is subject to appropriate approval.
- Comply with state and federal laws; CSU policies; and University standards, guidelines and procedures that govern access to and use of Level 1 confidential data and Level 2 internal use data, regardless of its format.
- Be sure that the most current anti-virus software is running on the computer since computer viruses can disrupt systems and destroy data.

Users may not:

- Disclose data to others, except as required by their job responsibilities.
- Use data for their own personal gain, nor for the gain or profit of others.
- Access data to satisfy their personal curiosity.
- Install or download software that is not approved by the University. There is a risk that the software could conflict with existing applications or may contain a virus. A list of software licensed by the University is available on the ITS website. For specific software questions, refer to the ITC authorized to install software for your department.

## 4.2 Data Security

Administrative data should be stored on secured network file servers, not on individual desktops, and never stored on a laptop or other portable device unless using a secured encryption method to secure the data.

To keep someone from gaining unauthorized access, either logout from the administrative information system before leaving a computer or restrict access by some other means (locked office/keyboard, desktop access control or a password-protected screen saver).

## 4.3 Requests for Release of Administrative Information

Requests for release of University administrative information must be referred to the data steward responsible for maintaining those data.

- Requests for student data must be directed to the University Registrar, Enrollment Services office, ADM 401.
- Requests for student directory information must be directed to the Office of Enrollment Services, ADM 146 or the Records Office, ADM 409.
- Requests for employee data must be directed to the assistant vice president for Human Resources Management, ADM 606.
- Requests for contributor data must be directed to the University Development office, ADM 802.
- Requests for data in decentralized systems must be directed to the appropriate division or department administrator.

## 4.4 Administrative Information System Access

All users accessing University administrative information systems must sign an *Access and Compliance* form, which is filed in the employee's official personnel file. Only one *Access and Compliance* form is required per individual and covers all systems that employee may access.

Administrators are to exercise discretion when authorizing employee access to University administrative information systems. Management must ensure that access to administrative information systems is revoked or modified as appropriate upon employee resignation, termination, job changes, or when grants or contracts expire.

## 4.5 Criteria for Authorization of an Administrative Information Systems Account

Individuals must meet the following criteria to obtain and hold an administrative information systems account:

a) Job duties legitimately require work that can be performed only by accessing the administrative information system(s).
b) Job duties require access to protected data.

c) Users must have taken the campus online FERPA tutorial and test (at http://www.calstatela.edu/its/itsecurity/ferpa), and have a signed FERPA certificate of completion on file with either the Human Resources Management office (for employees) or the Procurement and Contracts office (for vendors and consultants). A valid FERPA certificate of completion must be attached to the administrative information system account application, or the application must indicate that a FERPA certificate is already on file.

d) Users must sign an *Acknowledgment of Confidentiality* and *Appropriate Use of Account* agreement.

Access to one administrative information account does not automatically guarantee access to another administrative information system account.

## 4.6 Administrative Information Systems Accounts

Designated security administrators are the only personnel authorized to create, modify, unlock, revoke or un-revoke accounts in administrative information systems. Requests for new or modified administrative information system accounts must be reviewed and approved by each position listed below. By signing their approval, each approver affirms that the requestor's job duties and tasks legitimately require access to the specified administrative information system and the confidential information stored on it.

- Department chair/manager
- Dean/director
- Role owner(s)
- Data steward
- Director for IT Security and Compliance
- Vice president for Information Technology Services and CTO

To comply with segregation of duties requirements, system data stewards may never serve in the role of system security administrators.

### 4.6.1 Obtaining a New Account

To obtain a new account to an administrative information system users should go to http://www.calstatela.edu/its/services.php. Click on **CMS and Enterprise Applications** > **Forms** > select the system account request needed. When filling out the online form, the information provided will pre-populate an Adobe PDF file, which the requestor must print, sign and forward to the approvers as noted in that form's instruction sheet.

The request will be routed to the security administrators of the appropriate offices (e.g., SA security administrators for the SA system). The final approver's designated office staff will forward the completed request to the Human Resources Management office to file in the requestor's official personnel file. If the request is for a student assistant, it will be filed in the student's personnel file. For third-party service providers, the forms will be returned to the director for IT Security and Compliance for filing.

Returning part-time faculty who did not teach courses the previous quarter in the same department, as well as new part-time faculty, must submit a request for a new administrative information systems account.

### 4.6.2 Modifying an Account

To modify administrative information systems account users should go to http://www.calstatela.edu/its/services.php. Click on **CMS and Enterprise Applications** > **Forms** > and select the system modification application needed. When the request has been processed an e-mail is sent to the requestor indicating that the modification was completed.

### 4.6.3 Temporary Access

Temporary access is restricted to those programmer/analysts, consultants, functional users and technical users whose job duties and tasks legitimately require work that can be performed only by accessing the system for these reasons:

a) Troubleshooting and correcting application and system problems.
b) Implementing a new product, service or adjunct system.
c) Testing a new product, service or adjunct system.

Temporary access is limited to a maximum of six months and, with approval, two additional six-month extensions. If access is still required after the last extension expires, the requestor must re-apply for access.

The director for IT Security and Compliance shall send a calendar reminder to the appropriate security administrator with the expiration date of the temporary account.

### 4.6.4 Revoking an Administrative Information Systems Account Due to Separation or Special Request

Administrative information system accounts are revoked by ITS when it receives a separation notification from Human Resources Management or UAS-HR, or a special request from the University Counsel, the internal auditor, any system data steward or the office of the administrative function.

## 4.7 Passwords and User Login

The most effective way to protect administrative information is through the vigilant use of passwords. All administrative system users must follow the password standards outlined in *ITS-2008-S Password Standards*. Users are expected to treat their passwords as confidential and not share them with anyone. Every individual, including student employees, must have a unique user login.

### 4.7.1 New Accounts

**HR/SA/CR for Employees**: As soon as the request for a new account is processed, an automated e-mail is sent to the requestor or, for a student assistant account, to the student's supervisor, with instructions for picking up the password. Passwords may be retrieved at the ITS Help Desk after the ITS Help Desk staff verifies the requestor's or student supervisor's identity.

**HR/SA/CR for Student Assistants**: Student assistants may obtain an administrative information systems account for HR/SA/CR, but may NOT obtain a password. Supervisors are responsible for logging their student assistants into the administrative information system.

For new accounts, users must change their passwords upon first login to the administrative information system.

**CFS for Employees**: The Common Financial System account is linked with each user's *myCSULA Identity* account. As soon as the request for a new account is processed, an automated confirmation e-mail is sent to the requestor. Requestors can then access CFS through the *myCSULA Portal* with their *myCSULA Identity* user name and password.

**CFS for Student Assistants:** Student assistants may obtain an administrative information systems account for CFS. When student assistants are hired and their employee information is entered into HR, a new "staff" *myCSULA Identity* account is created. As soon as the request for a new account is processed, an automated confirmation e-mail is sent to the requestor. Student assistants can then access CFS through the *myCSULA Portal* with their *myCSULA Identity* user name and password.

> ***Note: To maintain proper system access security, it is imperative that departments submit the appropriate System Modification Request when student assistants separate from employment.***

### 4.7.2 Password Resets

Users can request an account password reset if they forget or lose their passwords, or their account was automatically locked after three (3) failed login attempts.

**For HR/SA/CR**: The security administrator will create a new password. An e-mail will be sent to the requestor or student assistant's supervisor with instructions for picking up the account password at the ITS Help Desk.

- To request an HR/SA password reset, either click on the previous link or go to the ITS home page > Faculty or Staff drop down menu at the top of the page > click on HR/SA Account Password Reset Form.
- To request a Contributor Relations password reset, either click on the previous link or go to the ITS home page > Browse All ITS Services > CMS and Enterprise Applications > Forms.

**For CFS**: The Common Financial System account is linked with each user's *myCSULA Identity* account.

- To request a Financials password reset, users must change their *myCSULA Identity* password at https://id.calstatela.edu/user/login.jsp.

## 5 Contacts

a) Address questions regarding these guidelines to: ITSecurity@calstatela.edu.

b) To report a security breach, contact the director for IT Security and Compliance at 323-343-2600 or e-mail itsecurity@calstatela.edu.

## 6 Applicable Federal and State Laws and Regulations

| Federal | Title |
|---|---|
| Family Educational Rights and Privacy Act (FERPA) | **Family Educational Rights and Privacy Act (FERPA)**<br>http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html<br>This is a federal law that protects the privacy of student education records. |
| Federal Privacy Act of 1974 | **Federal Privacy Act of 1974**<br>http://www.usdoj.gov/opcl/privacyact1974.htm<br>This is a federal act that establishes a code of fair information practices governing the collection, maintenance, use and dissemination of personally identifiable information about individuals that is maintained in systems of records by federal agencies. |
| Gramm-Leach-Bliley Act<br>15 USC, Subchapter 1, Sec. 6801-6809 | **Gramm-Leach-Bliley Act**<br>http://www.ftc.gov/privacy/glbact/glbsub1.htm<br>This is a federal law on the disclosure of non-public personal information. |
| **State** | **Title** |
| California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.85 | **California Civil Code Sections 1798.29, 1798.82, 1798.84, 1798.8**<br>http://www.leginfo.ca.gov/.html/civ_table_of_contents.html<br>This is a state law that, as amended by SB 1386 (2003), AB 1298 (2007) and SB 24 (2011), provides information on safeguarding personal information, requires notification to California residents whose personal information was or is reasonably believed to have been acquired by unauthorized individuals and requires notification to the Attorney General if more than 500 residents are involved. |
| SB 1386 | **California Personal Information Privacy Act, SB 1386**<br>http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.pdf<br>This bill modified Civil Code Section 1798.29 to require notification to individuals whose personal information is or is assumed to have been acquired by unauthorized individuals. |
| AB 1298 | **California Personal Information Privacy Act, AB 1298**<br>http://www.leginfo.ca.gov/pub/07-08/bill/asm/ab_1251-1300/ab_1298_bill_20071014_chaptered.pdf<br>This bill modified Civil Code Sections 1798.29 and 1798.82 to include medical and health information. |

| | |
|---|---|
| SB 24 | **California Personal Information Privacy Act, SB 24**<br>http://www.leginfo.ca.gov/pub/11-12/bill/sen/sb_0001-0050/sb_24_bill_20110831_chaptered.pdf<br>This bill modified Civil Code Section 1798.29 to require security breach notifications to fulfill certain additional requirements, including electronically submitting a single sample copy of the notification to the Attorney General when the security breach affects more than 500 California residents. |

## 7 Related Documents and Resources

| CSULA | Title |
|---|---|
| ITS-2524 | **Information Security Program for California State University, Los Angeles**<br>http://www.calstatela.edu/its/itsecurity/guidelines/Campus_Information_Security_Plan_2012.pdf<br>This document establishes the University's Information Security Program in support of its obligation to protect the technology resources and information assets entrusted to it. |
| Administrative Procedure 707 | **Records Retention, Management and Disposition**<br>http://www.calstatela.edu/univ/admfin/procedures/707/707.pdf<br>This procedure establishes policy for the secure management of University records and the transfer of University records to the State Records Center, the retrieval of stored records and the destruction of obsolete records. |
| ITS-1006-G | **User Guidelines for Securing Offices, Workspaces and Documents**<br>http://www.calstatela.edu/its/itsecurity/guidelines<br>This guideline helps the campus community protect offices, machines, devices and documents from unauthorized access to confidential, personal and proprietary information. |
| ITS-2008-S | **Password Standards**<br>http://www.calstatela.edu/its/itsecurity/guidelines<br>This standard provides guidance to all users regarding the security and management of passwords. |
| ITS-2812 | **Information Security Initial Incident Report**<br>http://www.calstatela.edu/its/forms/ITS-2812_InformationSecurityInitialIncidentReport.doc<br>Form used by departments to report an actual or suspected security incident to IT Security and Compliance. |
| ITS-6800 | **New Student Administration Account Request**<br>http://www.calstatela.edu/its/forms/get_account/<br>Form used to request a new SA account. |

| | |
|---|---|
| ITS-6801 | **Modification to Student Administration Account Request**<br>http://www.calstatela.edu/its/forms/get_account/indexmodsa.htm<br>This form is used to request a modification to, or revocation of, a user's current SA account. |
| ITS-6803 | **GET Student Administration Information System Access and Compliance Form (Staff)**<br>http://www.calstatela.edu/its/forms/get_account/<br>This form is automatically attached to the New Student Administration Account Request form submitted by a staff member. |
| ITS-6811 | **GET Student Administration Information System Access and Compliance Form (Faculty)**<br>http://www.calstatela.edu/its/forms/get_account/<br>This form is automatically attached to the New Student Administration Account Request form submitted by a faculty member. |
| ITS-6812 | **Financials Information System Account Request**<br>http://www.calstatela.edu/its/forms/get_account/indexfin.htm<br>Form used to request a new Financials account (also known as a Common Financial System (CFS) account). |
| ITS-6813 | **HR Information System Account Request**<br>http://www.calstatela.edu/its/forms/get_account/indexhr.htm<br>Form used to request a new HR account. |
| ITS-6814 | **Contributor Relations Information System Account Request**<br>http://www.calstatela.edu/its/forms/get_account/indexcr.htm<br>Form used to request a new Contributor Relations account. |
| ITS-6817 | **Modification to Human Resources Account Request**<br>http://www.calstatela.edu/its/forms/get_account/indexmodhr.htm<br>This form is used to request a modification to, or revocation of, a user's current HR account. |
| ITS-6823 | **Modification to Contributor Relations Account Request**<br>http://www.calstatela.edu/its/forms/get_account/indexmodcr.htm<br>This form is used to request a modification to, or revocation of, a user's current Contributor Relations account. |
| ITS-6824 | **Modification to Financials Account Request**<br>http://www.calstatela.edu/its/forms/get_account/indexmodfin.htm<br>This form is used to request a modification to, or revocation of, a user's current Financials account. |

| Chancellor’s Office | Title |
|---|---|
| ICSUAM 8000.0-8095.0 | **The California State University Information Security Policy and Standards**<br>http://www.calstate.edu/icsuam/sections/8000/<br>These documents provide policies and standards governing CSU information assets. |
| CSU Executive Order 1031 | **System-wide Records/Information Retention and Disposition Schedules Implementation**<br>http://www.calstate.edu/EO/EO-1031.html<br>http://www.calstate.edu/recordsretention<br>This Executive Order provides for the implementation of the California State University (CSU) System wide Records/Information Retention Schedules. |