 User Guidelines for Student Administration Access	Guidelines No.	ITS-1014-G	Rev:	C
	Owner:	IT Security Management and Compliance		
	Approved by:	Sheryl Okuno, Acting Director		
	Issued:	6/5/08	Effective:	6/5/08
	Page 1 of 6			

1 Purpose

The Student Administration (SA) system processes transactions and data pertaining to student educational records, such as academic advisement, admissions, financial aid, student financials, records, and recruiting. The SA system provides mission-critical functions and stores personal and confidential information. Therefore, access to it is strictly controlled and limited to only authorized personnel. These guidelines define the criteria for authorized SA access, and outline the required steps to obtain and maintain an SA account.

2 Definitions


FormTracker: An online campus system that tracks application requests through final approval

Role Owner: A data steward that has authority to define security roles in the SA system

3 Guidelines

3.1 Criteria for Obtaining an SA Account

- a) Access to confidential information is restricted and strictly controlled. Users who fail to meet the criteria below either will be denied an SA account or will have their existing SA account revoked immediately. Therefore, individuals must meet the following criteria to obtain and hold an SA account:
 - Job duties legitimately require work that can be performed only by accessing the SA system.
 - Job duties require access to personal and confidential information.
- b) As a prerequisite for obtaining an SA account, users must have taken the campus online FERPA tutorial and test (at <http://www.calstatela.edu/ferpa>), and have a signed FERPA certificate of completion on file with either the Human Resources Management office (for employees) or the Purchasing office (for vendors and consultants).
- c) Requests for new or modified SA 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 SA system and the confidential information stored in it:
 - Department Chair/Manager
 - Dean/Director
 - Role Owner(s)
 - Director of IT Security and Compliance
 - Vice President for Information Technology Services (ITS) and CTO
- d) Access to another confidential system does not automatically guarantee access to the SA system. Authorized users of other system who also require SA system access must apply and be approved for it.
- e) Users must apply for SA system access using the *New Student Administration Account Request* form, which includes an Acknowledgment of Confidentiality and Appropriate Use of Account agreement.

 User Guidelines for Student Administration Access	Guidelines No.	ITS-1014-G	Rev:	C
	Owner:	IT Security Management and Compliance		
	Approved by:	Sheryl Okuno, Acting Director		
	Issued:	6/5/08	Effective:	6/5/08
	Page 2 of 6			

- f) When applying for an SA account, requestors must also sign and submit a completed and management-approved faculty or staff *GET Student Administration Information System Access and Compliance Form*. This form is attached to the *New Student Administration Account Request* form.
- g) A valid FERPA certificate of completion must be attached to the SA account application, or the application must indicate that a FERPA certificate is already on file.

3.2 Criteria for Obtaining Temporary SA Access

- a) Temporary SA 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 SA system for these reasons:
 - Troubleshooting and correcting application and system problems
 - Implementing a new product, service, or adjunct system
 - Testing a new product, service, adjunct system
- b) 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.

3.3 Procedure for Obtaining or Modifying an SA Account

NOTE


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 Student Administration account as outlined below. Student assistants may obtain an SA account, but may NOT obtain a password. Supervisors are responsible for logging their student assistants into the SA system.

- a) For new accounts, users should apply online at <http://www.calstatela.edu/its/forms> ► **Student Administration** topic ► **Student Administration Account Request** link.

For account modifications, users should apply online at <http://www.calstatela.edu/its/forms> ► **Student Administration** topic ► **Student Administration Account Modification Request** link.

Directions are provided as the user steps through completing either form. An automated e-mail will send the requestor a Tracking Number and directions for accessing FormTracker. After obtaining the approval signatures of the Department Chair/Manager and the Dean/Director, the user must submit the form to the Registrar's Office.

- b) The designated staff in each of the following approver's offices will 1) log the request form in to FormTracker upon receipt, 2) log the form out of FormTracker upon approval, and 3) forward the form to the next approver:
 - Registrar's Office [Note: If approving, the Registrar must also obtain the approval signatures of any other necessary Role Owners and create a spreadsheet listing the appropriate security roles and profile templates that determine or modify this requestor's access to the SA system. The Registrar must e-mail the spreadsheet to the Director of IT Security and Compliance, and to an IT Security Analyst

 User Guidelines for Student Administration Access	Guidelines No.	ITS-1014-G	Rev:	C
	Owner:	IT Security Management and Compliance		
	Approved by:	Sheryl Okuno, Acting Director		
	Issued:	6/5/08	Effective:	6/5/08
	Page 3 of 6			

designated by the Director of IT Security and Compliance. The Registrar must also print the spreadsheet and attach to the request form before forwarding both to the IT Security and Compliance office.

- Director of IT Security and Compliance
- Vice President for Information Technology Services (ITS) and Chief Technology Officer (CTO)

The final approver's designated office staff will forward the completed request to the Human Resources Management office to file in the requestor's personnel file. If the request is for a student assistant or third party, the forms should be returned to the Director of IT Security and Compliance for filing.

- c) The designated IT Security Analyst shall perform a second-level request review, and shall e-mail the results to the SA Security Administrators.
- d) SA Security Administrators are the only personnel authorized to create, modify, unlock, revoke, or un-revoke accounts in the SA system. An SA Security Administrator shall create or modify accounts as specified in the IT Security Analyst's review. An SA Security Administrator also shall log the request's completion into the FormTracker system.
- e) For new accounts, as soon as the request is processed through the FormTracker system, 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 (LIB PW Lobby) after the ITS Help Desk staff verifies the requestor's or student supervisor's identity.

For modified accounts, as soon as the request is processed, an e-mail from the Enterprise Systems mailbox is sent to the requestor indicating that the modification was completed.


- f) For new accounts, users must change their passwords upon first login to the SA system.

3.4 Procedure for Obtaining Temporary SA Access

NOTE

Only requestors who meet the criteria defined in section 3.2 may request temporary SA access. Some requestors may already have another SA account, but need temporary access to a different portion of the SA system. These requestors will continue to use their normal SA usernames and passwords.

- a) Download the *Temporary PeopleSoft Administrative Account Request* from the ITS Forms website: <http://www.calstatela.edu/its/forms> ► **Student Administration** topic.
- b) On the form:
 1. Check the box(es) next to the database(s) you want to access.
 2. Describe the work that needs to be performed and why temporary access is necessary to perform it.
 3. Read, sign, and date the Acknowledgement of Confidentiality.
- c) Walk the form to the following offices to obtain these approval signatures:
 - Department chair or manager
 - Dean or Director

 User Guidelines for Student Administration Access	Guidelines No.	ITS-1014-G	Rev:	C
	Owner:	IT Security Management and Compliance		
	Approved by:	Sheryl Okuno, Acting Director		
	Issued:	6/5/08	Effective:	6/5/08
	Page 4 of 6			

- Registrar's Office
- d) Submit the form to the IT Security and Compliance office.
- e) The form will be circulated to the Director of IT Security and Compliance and the Vice President for ITS and CTO for approval.
- f) Upon approval, the Director of IT Security and Compliance will keep the original form and forward a copy to an SA Security Administrator to create the temporary account.

NOTE

The Director of IT Security and Compliance shall send a calendar reminder to the SA Security Administrator with the expiration date of the temporary account.

- g) Upon account creation, the SA Security Administrator shall e-mail the user to pick up the account information (username and password) at the ITS Help Desk, where the Golden Eagle Card or photo ID and CIN/proof of employment will be verified.

3.5 Procedure for an SA Account Password Reset


- a) Users should request an SA account password reset if:
 - They forget or lose their passwords, or
 - Their SA accounts were automatically locked after three (3) failed login attempts.
- b) From an Internet browser, go to <http://www.calstatela.edu/its/forms/pwreset.htm>. Enter all the information requested in the fields provided, and click the **Continue** button to submit the request.
- c) Once the request is submitted, the information is uploaded to a tracking database, a Tracking Number is assigned to the request, and an automated e-mail message is sent to the requestor with the Tracking Number and directions for accessing FormTracker.
- d) Upon receiving the request and verifying that this is a valid requestor and account, the SA Security Administrator will create a new SA password, and log the request's completion in the FormTracker system.
- e) Once the request is logged as processed, an automated e-mail is sent to the requestor or student assistant's supervisor with instructions for picking up the account password at the ITS Help Desk.
- f) Requestors or student assistant supervisors should bring their Golden Eagle Cards or photo IDs and proof of employment to the ITS Help Desk (LIB PW Lobby). ITS Help Desk staff must verify the requestor's or supervisor's identity and proof of employment before releasing the new password.

3.6 Procedure for Changing an SA Account Password

NOTE

This procedure does not apply to users who cannot remember or who lose their passwords or whose accounts have been locked due to three (3) failed login attempts.

- a) Log into your SA account.

 User Guidelines for Student Administration Access	Guidelines No.	ITS-1014-G	Rev:	C
	Owner:	IT Security Management and Compliance		
	Approved by:	Sheryl Okuno, Acting Director		
	Issued:	6/5/08	Effective:	6/5/08
	Page 5 of 6			

- b) Under **Menu** (on the right side of the screen), click on **Change My Password**.
- c) In the **Current Password** field, enter your existing password.
- d) In the **New Password** field, enter the new password.
- e) In the **Confirm Password** field, enter the new password again.
- f) Click the **Change Password** button to apply the new password to the account.

3.7 Revoking an SA Account Due to Separation or Special Request


- a) SA 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 University Auditor, or the Registrar’s Office.
- b) When SA account holders are transferred, promoted, or otherwise assume different job duties and tasks that no longer require SA access or that require different SA access, a *Modification to Student Administration Account Request* form must be submit as outlined in section 3.3.

3.8 Requests to “Un-revoke” an SA Account

If any user’s SA account was revoked due to separation, special request, or an instruction on a *Modification to Student Administration Account Request* form, that account cannot be “un-revoked.” Instead, if that user needs SA access, he or she must meet all the criteria as listed in section 3.1 and must reapply for a new SA account according to the procedure outlined in section 3.3.

4 Terms, Conditions, and Sanctions

- a) To become an authorized SA system user, requestors must sign the Acknowledgment of Confidentiality and Appropriate Use of Account agreement that is part of the *GET Student Administration (SA) Account Request* form.
- b) All users must abide by all the terms and conditions of any and all University confidentiality agreements they sign. Any violations of confidentiality will result in immediate account revocation.
- c) Users are expected to treat their User IDs and passwords as confidential and not share them with anyone.
- d) All users must comply with the state and federal laws and University policies that govern access to, and use of, confidential information, regardless of its format.
- e) A violation of information security precautions may be a crime and may result in any legal and disciplinary actions that apply, including criminal prosecution.
- f) If there is reason to believe a violation of federal or state law, or University information security practices, guidelines, or policies occurred using an SA account, that account and account contents may be subject to monitoring and examination by authorized personnel.
- g) All University employees and contractors are subject to California Government Code section 8314, which addresses the use of public resources for unauthorized purposes.

 User Guidelines for Student Administration Access	Guidelines No.	ITS-1014-G	Rev:	C
	Owner:	IT Security Management and Compliance		
	Approved by:	Sheryl Okuno, Acting Director		
	Issued:	6/5/08	Effective:	6/5/08
	Page 6 of 6			

- h) All University employees and contractors are subject to California Penal Code sections 502 and 502.01, which deal with unauthorized access to computers, computer systems, computer data, and the criminal penalties that apply for violations.
- i) SA users must take the FERPA tutorial and test every two years, and file a current FERPA certificate of completion with either the Human Resources Management office (for employees) or the Purchasing office (for vendors and consultants).

5 Contacts and Resources

- a) For questions regarding these user guidelines, contact ITSecurity@calstatela.edu.
- b) For FormTracker system technical support, contact the IT Help Desk, LIB PW Lobby, (323) 343-6170.
- c) Links to applicable laws, regulations, and user guidelines are located on the ITS Guidelines and Policies Web site at <http://www.calstatela.edu/its/policies>.
- d) Any security breaches or violations of campus or remote CMS databases should be reported by telephone within fifteen minutes of discovery to the individuals listed below. A written follow-up minimally containing the date, time, event, emergency contact personnel, emergency contact phone number, system impact, user impact, current actions, and planned actions, must be e-mailed to the same individuals within four hours of discovery.

Vice President for ITS and CTO Phone: 323-343-2600 ITSecurity@calstatela.edu	Director of IT Security and Compliance Phone: 323-343-2600 ITSecurity@calstatela.edu
-----------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------

6 Related Documents

ID/Control #	Title
ITS-6811	GET Student Administration Information System Access and Compliance Form (Faculty) Form that is automatically attached to the New Student Administration Account Request form submitted by a faculty member http://www.calstatela.edu/its/forms/get_account/
ITS-6803	GET Student Administration Information System Access and Compliance Form (Staff) Form that is automatically attached to the Student Administration Account Request form submitted by a staff member http://www.calstatela.edu/its/forms/get_account/
ITS-6801	Modification to Student Administration Account Request Form used to request a modification to, or revocation of, a user's current SA account. http://www.calstatela.edu/its/forms/get_account/indexmodsa.htm
ITS-6800	New Student Administration Account Request Form used to request a new SA account http://www.calstatela.edu/its/forms/get_account/
ITS-2801	Temporary PeopleSoft Administrative Account Request Form used to request temporary access to the SA system http://www.calstatela.edu/its/forms/ (Student Administration topic)