Administrative Systems Access Controls and Segregation of Duties Review

Procedure No.	ITS-2007-P	Rev:	A
Owner:	IT Security and Compliance		
Approved by:	Sheryl Okuno, Director IT Security and Compliance		
Issued:	4-16-09	Revised:	12-20-12
			Page 1 of 17

Table of Contents

1 General Scope and Responsibilities

It is the intent of California State University, Los Angeles (CSULA) to have proper PeopleSoft security access and Segregation of Duty controls in place for its Common Management Systems (CMS) and to ensure that access controls are consistently implemented and enforced. To manage this requirement, the University created this formalized procedure to ensure that constituents are aware of the requirements, responsibilities and reporting necessary to maintain these controls.

The CSULA Contributor Relations system is currently not incorporated in the CMS system, but is run locally on the campus. However, since Contributor Relations must withstand periodic security audits, the University intends to perform the identical security reports, reviews and remediations required of the CMS systems.

2 Entities Affected by this Procedure

This procedure applies to all individuals at CSULA who administer systems with PeopleSoft Access Controls and must maintain adequate Segregation of Duties. This procedure also applies to all individuals responsible for the supervision, review and reporting of periodic access control audits.

3 Definitions

a) Access Controls: The ability to permit or deny the use of a particular resource by a particular entity, generally by administering permissions or access rights to specific users or groups of users. These permission or access rights control the user’s ability to view or make changes to the contents of the system.

b) Common Financial System (CFS): A component of the CSU Common Management System (CMS) that contains accounts payable, accounts receivable, billing, asset management, general ledger and purchasing.

c) Common Management System (CMS): The CSU best practices approach to support human resources, financials and student services administration functions with a common suite of Oracle Enterprise applications in a shared data center, with a supported data warehouse infrastructure.

d) Contributor Relations (CR): A campus-based administrative system that manages charitable contributions from donors and alumni.

e) Database Administrator: A person responsible for the physical design and/or management of the database.

f) Human Capital Management (HCM): A component of the CSU Common Management System (CMS) that contains the student administration and human resources administrative systems. The student administration (SA) component includes academic advisement, admissions, campus community, financial aid, student financials, student records and student self-service. The human resources (HR) component includes absence management, benefits administration, labor cost distribution, acquisition manager, temporary faculty, time and labor, workforce administration, position management, regulatory requirements and personnel self-service.

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

h) Segregation of Duties: A security principle that has as its primary objective the prevention of fraud and errors.

i) System Data Steward: An individual who has management responsibilities (e.g., planning, policy, etc.) for defined segments of the University data as it relates to their functional operations.

4 Requirements

4.1 Access Control Requirements

CSULA must maintain approved security controls and procedures that meet the Chancellor's Office audit requirement to identify inappropriate access and segregation of duties conflicts. Key areas of concern are security administrators, database administrators and analyst/programmer classification employees with access to one or more of the following:

- Delivered PSADMIN
- Maintain Security
- Administer Security
- Application Designer
- Data Mover
- Database Role CSU_UPDATE
- Database Role DBA

For the HCM and CR systems, these roles may be applied to security administrators, database administrators and programmers.

For the CFS system, these roles should never be applied to campus security administrators, database administrators or programmers since these roles are the responsibility of CMS Central Security.

These roles must never be applied to campus users' access.

4.2 Personnel Requirements

Designated University employees must maintain ongoing oversight of access controls to ensure that employees granted these access controls remain compliant with appropriate access and avoid segregation of duties conflicts. The results of these monthly tests must be reviewed and remediated immediately, if necessary. A certified report must be submitted to the Chancellor's Office annually. The following identifies these designated responsibilities:

Role/Title	Responsibility
Database Administrator for Contributor Relations	a) Runs the monthly testing scripts cited in section 5.2.1.6. b) Submits the script results to the director for CMS and Enterprise Systems.
Database Administrator for HCM (Campus Technical Users Group (TUG) representative)	a) Receives monthly notifications from CMS Central that the reports cited in section 5.2.1.3 are available for download. b) Downloads the reports and sends to the director of IT Security and Compliance.

Role/Title	Responsibility
Database Administrator for CFS (Campus Technical Users Group (TUG) representative)	a) Receives monthly notifications from CMS Central that the reports cited in section 5.1.2.1 (paragraph B) are available for download. b) Downloads the reports and sends to the director of IT Security and Compliance.
Director of CMS and Enterprise Systems	a) Ensures that the testing scripts cited in section 5.2.1.6 are run quarterly by the Contributor Relations database administrator. b) Submits preliminary test results to the director of IT Security and Compliance for internal review. c) Submits final test results to the University internal auditor. d) Initiates corrective measures for non-compliant findings. e) Submits final documentation of corrective actions and remediation measures to the University internal auditor.
Director of for Administrative Technology	a) Works with the appropriate personnel to resolve non-compliant access controls or lack of segregation of duties issues.
Director of IT Security and Compliance	a) Reviews the CMS Central and campus-prepared monthly reports cited in sections 5.2.1.1. (paragraph B), 5.2.1.1 5.2.1.3 and 5.2.1.6. b) Performs internal ITS review of preliminary test results. c) Retains campus corrective action tests and documentation for twelve months. d) In coordination with the University controller, prepares and submits the annual *Review of PS Access Controls/Segregation of Duties Summary of Exceptions Report* and *Certification of Annual Systems Access Review* to the vice presidents for Information Technology Services and Administration. e) Retains the annual *Review of PS Access Controls/Segregation of Duties Summary of Exceptions Report* and *Certification of Annual Systems Access Review* for five years.

Role/Title	Responsibility
System Data Stewards	a) Reviews account access forms with segregation of duties in mind when granting system security access. b) Works with the University internal auditor to resolve non-compliant access controls and/or to seek an exception. c) Notifies employees when non-compliant access controls or lack of segregation of duties requires modification or termination of access.
University Internal Auditor	a) Reviews and validates quarterly testing script results for compliance. b) Reports non-compliant findings to the vice presidents for ITS/CTO and/or Administration. c) Reports non-compliant findings to the appropriate data steward. d) Opens corrective action cases with the director of CMS and Enterprise Systems or director of Administrative Technology, as appropriate. e) Works with system data stewards to develop exception requests when a non-compliance issue cannot be resolved. f) Submits the signed *Certification of Annual Systems Access Review* to the Chancellor's Office.
University Controller	a) Reviews the CMS Central monthly CFS three-way match report cited in section 5.2.1.1 B. b) Reports non-compliant findings to the University internal auditor. c) In coordination with the director for IT Security and Compliance, prepares and submits the annual *Review of PS Access Controls/Segregation of Duties Summary of Exceptions Report* and *Certification of Annual Systems Access Review* to the vice presidents for Information Technology Services and Administration. d) Submits the signed *Certification of Annual Systems Access Review* to the University internal auditor.

Role/Title	Responsibility
Vice President for Administration and Finance/CFO	a) Reviews and signs the yearly *Certification of Annual Systems Access Review*, and returns it to the University controller.
Vice President for Information Technology Services/CTO	a) Reviews and signs the yearly *Certification of Annual Systems Access Review,* and returns it to the University controller.

4.3 DBA and Security Administrator Account Application Requirements

Any individual who requires permanent or temporary database administrator (DBA) and system security administrator access must adhere to the procedures and privileges outlined in *ITS-1012-G User Guidelines for Oracle Access*.

5 Procedures

This section describes the scripts and instructions; specific procedures for scheduling tests; verifying test results; exception monitoring and notification; documentation requirements; and error mitigation.

5.1 Instructions for Preparing Test Scripts

There are seven test scripts, indicated in the table below, that must be run monthly in the CFS and HCM environments and quarterly in the CR environment.

- **CFS**. CMS Central is responsible for running the segregation of duties scripts (Three-way Match and Maintain Security) for CFS and providing the results to the database administrator who forwards a copy of the reports to the director of IT Security and Compliance.
- **HCM**. CMS Central is responsible for running all the segregation of duties scripts for HCM and providing the results to the database administrator who forwards a copy of the reports to the director of IT Security and Compliance.
- **CR**. The director for CMS and Enterprise Systems is responsible for ensuring the CR database administrator runs the scripts, the results are verified for accuracy and a preliminary report copy sent to the director of IT Security and Compliance for internal review. Following the internal review, the reports are distributed to the University internal auditor.

Testing Script Title	Instructions
kpmg_chk_3way_match.sql *Lists operators with the ability to override the 3-way match rules.*	REM CHECK 3-WAY MATCH RULES. REM TO BE RUN IN A FINANCE APPLICATION ENVIRONMENT. SET LINESIZE 1000 SELECT DISTINCT A.OPRID, A.OPRDEFNDESC, D.MENUNAME, D.BARNAME, D.BARITEMNAME, D.PNLITEMNAME FROM SYSADM.PSOPRDEFN A, SYSADM.PSROLEUSER B, SYSADM.PSROLECLASS C, SYSADM.PSAUTHITEM D, SYSADM.PS_OPR_DEF_TBL_AP E WHERE A.OPRID = B.ROLEUSER

Testing Script Title	Instructions
	AND B.ROLENAME = C.ROLENAME AND C.CLASSID = D.CLASSID AND A.OPRID = E.OPRID AND A.ACCTLOCK = '0' AND E.AUTH_OVRRD_MATCH = 'Y' AND D.BARITEMNAME LIKE 'MATCH%' AND D.DISPLAYONLY = '0';

kpmg_chk_dba_dbm.sql
Lists users with Database Administrator rights.
This will be excluded from the campus check of Contributor Relations.
	SET LINE SIZE 1000
	SELECT DISTINCT A.USERNAME, A.GRANTED_ROLE
	FROM (select c.name dbname, a.username, b.granted_role from dba_users a, dba_role_privs b, v$database c where a.username=b.grantee) A
	WHERE
	A.USERNAME not in ('JLIN','MGARIA','COLSON','CWOODS','DDANG','GMANSOOR','HIEN','HLEE','JCHUAYCHAM','JGONZALEZ','JTRAN','KNGO','KNGUYEN','MCHING','SYS','OPS$ORACLE','SYSADM','SYSTEM'
	,'UNISYS_DBA','NNGO','RKAKULAWARAM','RVELLANKI','TNGO','JBALDONADO','JKIM','MGARIA','RHYUN')
	AND (A.GRANTED_ROLE='CSU_UPDATE' Or A.GRANTED_ROLE='DBA');

kpmg_chk_datamover.sql
Lists users with the ability to run scripts via DataMover.
	SET LINE SIZE 1000
	SELECT DISTINCT PSOPRDEFN.OPRID, PSOPRDEFN.OPRDEFNDESC, PSAUTHITEM.MENUNAME, PSAUTHITEM.AUTHORIZEDACTIONS, PSROLEDEFN.ROLESTATUS, PSAUTHITEM.DISPLAYONLY, PSOPRDEFN.ACCTLOCK, PSAUTHITEM.CLASSID, PSROLECLASS.ROLENAME
	FROM ((PSAUTHITEM INNER JOIN PSROLECLASS ON PSAUTHITEM.CLASSID = PSROLECLASS.CLASSID) INNER JOIN PSROLEDEFN ON PSROLECLASS.ROLENAME = PSROLEDEFN.ROLENAME) INNER JOIN (PSOPRDEFN INNER JOIN PSROLEUSER ON PSOPRDEFN.OPRID = PSROLEUSER.ROLEUSER) ON PSROLEDEFN.ROLENAME = PSROLEUSER.ROLENAME
	WHERE (((PSAUTHITEM.MENUNAME)='DATA_MOVER') AND ((PSROLEDEFN.ROLESTATUS)='A') AND ((PSAUTHITEM.DISPLAYONLY)<>'1') AND ((PSOPRDEFN.ACCTLOCK)<>'1'));

kpmg_chk_maintain_security.sql
Lists users with access the maintain security component of PeopleSoft.
	SET LINE SIZE 1000
	SELECT DISTINCT PSOPRDEFN.OPRID, PSOPRDEFN.OPRDEFNDESC, PSAUTHITEM.MENUNAME, PSROLEDEFN.ROLESTATUS, PSAUTHITEM.BARNAME, PSOPRDEFN.ACCTLOCK, PSAUTHITEM.DISPLAYONLY, PSAUTHITEM.PNLITEMNAME, PSAUTHITEM.CLASSID, PSROLEUSER.ROLENAME
	FROM ((PSAUTHITEM INNER JOIN PSROLECLASS ON PSAUTHITEM.CLASSID = PSROLECLASS.CLASSID) INNER JOIN PSROLEDEFN ON PSROLECLASS.ROLENAME = PSROLEDEFN.ROLENAME) INNER JOIN (PSROLEUSER INNER JOIN PSOPRDEFN ON PSROLEUSER.ROLEUSER = PSOPRDEFN.OPRID) ON PSROLEDEFN.ROLENAME = PSROLEUSER.ROLENAME
	WHERE (((PSAUTHITEM.MENUNAME)='MAINTAIN_SECURITY') AND ((PSROLEDEFN.ROLESTATUS)='A') AND ((PSAUTHITEM.BARNAME)<>'INQUIRE' And (PSAUTHITEM.BARNAME)<>'REPORT') AND

Testing Script Title	Instructions
	((PSOPRDEFN.ACCTLOCK)<>'1') AND ((PSAUTHITEM.DISPLAYONLY)<>'1') AND ((PSAUTHITEM.PNLITEMNAME)<>'EMAIL_PSWD' And (PSAUTHITEM.PNLITEMNAME)<>'EMAIL_CONFIRM' And (PSAUTHITEM.PNLITEMNAME)<>'SINGLE_SIGNON' And (PSAUTHITEM.PNLITEMNAME)<>'ADMINISTER_CERTS' And (PSAUTHITEM.PNLITEMNAME)<>'PSWD_CHNG_CNFRM' And (PSAUTHITEM.PNLITEMNAME)<>'PSPSWDHINT' And (PSAUTHITEM.PNLITEMNAME)<>'CHANGE_PASSWORD' And (PSAUTHITEM.PNLITEMNAME)<>'USER_SELF_SERVICE' And (PSAUTHITEM.PNLITEMNAME)<>'PSTREEMGRACC' And (PSAUTHITEM.PNLITEMNAME)<>'PSTREEMGRACCSRCH' And (PSAUTHITEM.PNLITEMNAME)<>'PSTREEMGRXFER' And (PSAUTHITEM.PNLITEMNAME)<>'PLIST_QUERIES' And (PSAUTHITEM.PNLITEMNAME)<>'ROLE_AUDIT' And (PSAUTHITEM.PNLITEMNAME)<>'ROLE_QUERY' And (PSAUTHITEM.PNLITEMNAME)<>'RUN_QRYACCLIST' And (PSAUTHITEM.PNLITEMNAME)<>'USER_QUERY'));
kpmg_chk_admin_security.sql *Lists users with the ability to grant business unit security and module-specific security. This doesn't include access to Maintain Security.*	SET LINE SIZE 1000 SELECT DISTINCT PSOPRDEFN.OPRID, PSOPRDEFN.OPRDEFNDESC, PSAUTHITEM.MENUNAME, PSOPRDEFN.ACCTLOCK, PSAUTHITEM.DISPLAYONLY, PSROLEDEFN.ROLESTATUS, PSAUTHITEM.PNLITEMNAME, PSROLECLASS.CLASSID, PSROLECLASS.ROLENAME, PSAUTHITEM.BARNAME FROM ((PSAUTHITEM INNER JOIN PSROLECLASS ON PSAUTHITEM.CLASSID = PSROLECLASS.CLASSID) INNER JOIN PSROLEDEFN ON PSROLECLASS.ROLENAME = PSROLEDEFN.ROLENAME) INNER JOIN (PSROLEUSER INNER JOIN PSOPRDEFN ON PSROLEUSER.ROLEUSER = PSOPRDEFN.OPRID) ON PSROLEDEFN.ROLENAME = PSROLEUSER.ROLENAME WHERE (((PSAUTHITEM.MENUNAME)='ADMINISTER_SECURITY') AND ((PSOPRDEFN.ACCTLOCK)<>'1') AND ((PSAUTHITEM.DISPLAYONLY)<>'1') AND ((PSROLEDEFN.ROLESTATUS)='A') AND ((PSAUTHITEM.PNLITEMNAME)<>'EMAIL_PSWD' And (PSAUTHITEM.PNLITEMNAME)<>'CHANGE_PASSWORD' And (PSAUTHITEM.PNLITEMNAME)<>'USER_SELF_SERVICE') AND ((PSAUTHITEM.BARNAME)<>'INQUIRE' And (PSAUTHITEM.BARNAME)<>'REPORT'));
kpmg_chk_psadmin.sql *Lists users with the PeopleSoft Administrator role.*	SET LINE SIZE 1000 SELECT DISTINCT PSOPRDEFN.OPRID, PSOPRDEFN.OPRDEFNDESC, PSROLECLASS.CLASSID, PSOPRDEFN.ACCTLOCK, PSROLEDEFN.ROLESTATUS, PSROLEUSER.ROLENAME FROM PSROLEDEFN INNER JOIN ((PSROLECLASS INNER JOIN PSROLEUSER ON PSROLECLASS.ROLENAME = PSROLEUSER.ROLENAME) INNER JOIN PSOPRDEFN ON PSROLEUSER.ROLEUSER = PSOPRDEFN.OPRID) ON PSROLEDEFN.ROLENAME = PSROLECLASS.ROLENAME WHERE (((PSROLECLASS.CLASSID)='PSADMIN') AND ((PSOPRDEFN.ACCTLOCK)<>'1') AND ((PSROLEDEFN.ROLESTATUS)='A'));

Testing Script Title	Instructions

kpmg_chk_app_designer.sql
Lists users with Application Designer Write access.
	SET LINE SIZE 256
	SELECT DISTINCT PSOPRDEFN.OPRID, PSOPRDEFN.OPRDEFNDESC, PSAUTHITEM.MENUNAME, PSAUTHITEM.AUTHORIZEDACTIONS, PSROLEDEFN.ROLESTATUS, PSAUTHITEM.DISPLAYONLY, PSOPRDEFN.ACCTLOCK, PSAUTHITEM.BARNAME, PSAUTHITEM.CLASSID, PSROLECLASS.ROLENAME
	FROM ((PSAUTHITEM INNER JOIN PSROLECLASS ON PSAUTHITEM.CLASSID = PSROLECLASS.CLASSID) INNER JOIN PSROLEDEFN ON PSROLECLASS.ROLENAME = PSROLEDEFN.ROLENAME) INNER JOIN (PSOPRDEFN INNER JOIN PSROLEUSER ON PSOPRDEFN.OPRID = PSROLEUSER.ROLEUSER) ON PSROLEDEFN.ROLENAME = PSROLEUSER.ROLENAME
	WHERE (((PSOPRDEFN.OPRID)<>'SOSSTECH' And (PSOPRDEFN.OPRID)<>'CMSETS') AND ((PSAUTHITEM.MENUNAME)='APPLICATION_DESIGNER') AND ((PSROLEDEFN.ROLESTATUS)='A') AND ((PSAUTHITEM.DISPLAYONLY)<>1) AND ((PSOPRDEFN.ACCTLOCK)<>1)) AND PSAUTHITEM.AUTHORIZEDACTIONS=4;

5.2 Instructions for Running Scripts and Verifying Results

5.2.1 Compensation Controls

Scripts will be run on a monthly basis as a compensating control to identify any unauthorized changes to User Access, Permissions Lists and/or Roles made by any individuals who have both Maintain Security and Administer Security roles. For the centralized CFS and HCM systems, this is a shared responsibility between CMS Central and the campus. For the CR system, the campus bears sole responsibility.

5.2.1.1 CMS Central Responsibilities in the Common Financial Systems (CFS)

A. CMS Central will run the following scripts on a monthly basis. Changes reported on these are controlled by the Chancellor's Office CFS Security Administration Team. Results will be reviewed by the CFS Security Administration Team.

Script Title	Report
CSUSEC02	Unassigned Permission List
CSUSEC03	Unassigned Roles
CSUSEC07	Permission List Modified
CSUSEC08	Roles Modified
CHK_MAINTAIN_SECURITY	Maintain Security Access

B. CMS Central will also run the following scripts on a monthly basis and will notify the campus database administrator when the reports are available for download. These scripts are maintained by CMS Central to be campus-specific.

System(s)	Script Title	Report
CFS ONLY	CHK_3WAY_MATCH	Users with Three-way Override
CFS & HCM	CHK_MAINTAIN_SECURITY	Users with Maintain Security Access
HCM	CHK_ADMIN_SECURITY	Users with Ability to Grant Security
HCM	CHK_APP_DESIGNER	Users with Application Designer Write Access
HCM	CHK_DATAMOVER	Users with Ability to Run Scripts
HCM	CHK_DBA_DBM	Users Database Administrator Rights
HCM	CHK_PSADMIN	Users with System Administrator Role

5.2.1.2 Campus Responsibilities in the Common Financial Systems (CFS)

A. The campus has no responsibility related to the following reports since they are controlled by the Chancellor’s Office CFS Security Administration Team:

- CSUSEC02 Unassigned Permission List
- CSUSEC03 Unassigned Roles
- CSUSEC07 Permission List Modified
- CSUSEC08 Roles Modified

B. Upon notification from CMS Central that the following monthly reports are ready, the database administrator will download the reports and e-mail them to the director for IT Security and Compliance. The director of IT Security and Compliance will forward a copy of the three-way match report to the University controller. The University controller is responsible for reviewing the users with three-way match report monthly. The director of IT Security and Compliance is responsible for reviewing the remainder of the reports monthly:

- (CFS ONLY) CHK_3WAY_MATCH Users with Three-way Override
- (CFS & HCM) CHK_MAINTAIN_SECURITY Users with Maintain Security Access
- (HCM) CHK_ADMIN_SECURITY Users with Ability to Grant Security
- (HCM) CHK_APP_DESIGNER Users with Application Designer Write Access
- (HCM) CHK_DATAMOVER Users with Ability to Run Scripts
- (HCM) CHK_DBA_DBM Users Database Administrator Rights
- (HCM) CHK_PSADMIN Users with System Administrator Role

C. The following reports should be run by the campus CMS and Enterprise Systems security administrator and reviewed on an as needed basis by the director of CMS and Enterprise Systems and when changes have been made to the system including, but not limited to 1) release upgrades; 2) changes to security roles; and 3) changes made to permission lists or profiles:

Script Title	Report
CSUSEC01	Locked Accounts
CSUSEC04	Operator IDs and Assigned Roles
CSUSEC05	Role, Permission List and Pages
CSUSEC06	User Modified Report
CSUSEC10	Operator IDs and Preferences

5.2.1.3 CMS Central Responsibilities in Human Capital Management (HCM)

CMS Central will run the following scripts on a monthly basis and will notify the campus database administrator when the reports are available for download. These scripts are maintained by CMS Central to be campus-specific:

System(s)	Script Title	Report
CFS & HCM	CHK_MAINTAIN_SECURITY	Users with Maintain Security Access
HCM	CHK_ADMIN_SECURITY	Users with Ability to Grant Security
HCM	CHK_APP_DESIGNER	Users with Application Designer Write Access
HCM	CHK_DATAMOVER	Users with Ability to Run Scripts
HCM	CHK_DBA_DBM	Users Database Administrator Rights
HCM	CHK_PSADMIN	Users with System Administrator Role

5.2.1.4 Campus Responsibilities in Human Capital Management (HCM)

There is no current need for compensating controls in HCM because the system has no issues related to segregation of duties. In the event the monthly “kpmg” scripts identify individuals who have and require both Maintain Security and Administer Security roles in HCM, an acceptable compensating control will be developed by the University internal auditor to review for inappropriate activities.

5.2.1.5 CMS Central Responsibilities in Contributor Relations (CR)

Contributor Relations is a campus-based system and CMS Central has no responsibilities for the CR system.

5.2.1.6 Campus Responsibilities in Contributor Relations (CR)

It is the responsibility of the director for CMS and Enterprise Systems to ensure the following scripts are run monthly by the database administrator for Contributor Relations, the results are verified for accuracy and a preliminary report copy sent to the director of IT Security and Compliance for internal review.

Script Title	Report
CHK_DBA_DBM	Database Administrator Rights
CHK_DATAMOVER	Users with Ability to Run Scripts
CHK_MAINTAIN_SECURITY	ITS Security Administrators
CHK_ADMIN_SECURITY	Users with Ability to Grant Security
CHK_PSADMIN	System Administrator Role
CHK_APP_DESIGNER	Users with Application Designer Write Access

5.3 Instructions for Processing Exceptions

5.3.1 Non-compliance Reporting

In the event the testing reports show that the access controls are non-compliant, the University internal auditor, the director of IT Security and Compliance, or the University controller will promptly report the issue in writing to the appropriate vice president or his/her designee and the system data steward. The non-compliance report must minimally contain the following information:

- Exact nature of the non-compliance;
- Date discovered;
- Estimate on the duration of time that the condition may have existed;
- System data steward’s explanation for why that access was provided, if known; and
- Remediation actions and estimated time required to remediate.

5.3.2 Requesting an Exception

In situations where a non-compliant issue cannot be resolved, the University internal auditor will contact the functional data steward to determine appropriate mitigation procedures. If an exception is required, the request must be submitted in writing and approved by the director of IT Security and Compliance and the vice president for Information Technology Services. Exception requests must include a plan for testing the exception measure to assure ongoing compliance. All approved exception requests are maintained by the director of IT Security and Compliance and may be requested for future audit submissions.

5.4 Mitigation Procedures

In the event corrective measures are required, the University internal auditor will open a case with the director of IT Security and Compliance and the director of CMS and Enterprise Systems to track and record the remediation of the exception. The director of IT Security and Compliance will notify specific parties involved with research and remediation efforts concerning the non-compliancy finding. A root cause analysis will be conducted by the directors and a solution will be implemented to mitigate the issue.

5.5 Documentation Requirements

All corrective measures and the procedures taken to remediate the identified problem must be documented on the *Summary of Exceptions* template provided by the Chancellor’s Office. The director of CMS and Enterprise Systems must submit this document to the director of IT Security and Compliance.

5.6 Documentation Retention Period

5.6.1 Summary of Exceptions

Corrective measures documented in the *Summary of Exceptions* template and evidence of the exception and resolution process will be maintained for a minimum of twelve months by the director of IT Security and Compliance.

5.6.2 Review of PS Access Controls/Segregation of Duties Summary Report

The annual test and remediation summary report will be maintained for a minimum of five years by the director of IT Security and Compliance.

5.6.3 Certification of Annual Systems Access Review

A signed copy of the annual certification will be maintained for a minimum of five years by the director of IT Security and Compliance.

5.7 Reporting Requirements

5.7.1 Review of PS Access Controls/Segregation of Duties Summary of Exceptions Report

An annual *Review of PS Access Controls/Segregation of Duties Summary of Exceptions Report* will be prepared jointly by the University controller and the director of IT Security and Compliance. The completed report will be delivered to the vice president for Administration and the vice president for Information Technology Services for their review. Following review and approval, the report is returned to the University internal auditor for submission to the Chancellor’s Office, and an official campus copy is retained by the director for IT Security and Compliance.

5.7.2 Certification of Annual Systems Access Review

A *Certification of Annual Systems Access Review* signed jointly by the vice president for Administration and the vice president for Information Technology Services will be submitted annually to the University internal auditor. The University internal auditor is responsible for submitting it to the appropriate Chancellor’s Office recipient, and an official campus copy is retained by the director of IT Security and Compliance.

6 Quality Assurance Provisions

6.1 Customer Relations Management

In the event that non-compliant or conflict-of-interest access rights are discovered, the director of IT Security and Compliance or the University internal auditor, as deemed appropriate, is responsible for notifying that employee (or employee’s supervisor) whose access is being modified or terminated of the intended action. If a new account access form is submitted to correct the non-compliant access, priority action should be taken to provide the corrected access as soon as possible.

6.2 Configuration Management

Not applicable to this procedure.

6.3 Change Management

Due to the critical nature of CMS Access Controls and the strict requirements for segregation of duties, no system administrator, security administrator, database administrator or other individual with these high level access rights shall create or modify any employee's access rights without a fully reviewed and approved system access form. The original copy of all approved access forms is filed in the employees' official personnel file in Human Resources Management.

6.4 Disaster Recovery/Business Continuity Management

Copies of reports and certifications that must be retained must be securely stored in such a manner as to be retrievable in the event of a disaster or loss of campus systems. If reports are stored electronically, there must be a secured backup copy.

6.5 Security Management

Test results are confidential and must never be shared beyond those employees authorized by position descriptions to view them. Test results, remediation documents and annual reports are not to be removed from the campus unless they are being stored at an approved records retention/storage facility.

6.6 Accounting Management

Documentation created by this procedure falls into the categories of both audit management and records retention management. To meet audit management requirements, test procedures, test results and remediation actions must be documented and retained for a minimum of twelve months. To meet records retention management requirements, the annual *PS Access Controls/Segregation of Duties Summary of Exceptions* Report and annual *Certification of Annual Systems Access Review* must be securely retained for a minimum of five years.

6.7 Fault Management

While the quarterly tests are intended to identify and correct access control problems, all individuals with system administrator, security administrator, or database administrator rights are expected to be vigilant when identifying potential access control or segregation of duties conflicts. These potential conflicts should be reported immediately to the director of IT Security and Compliance for assessment and action.

6.8 Efficiency/Effectiveness Management

The effectiveness of this procedure can be measured by the number of non-compliant findings discovered each quarter. It is the intent of CSULA to have no-findings test results each quarter. Failure to meet this expectation will require an evaluation of current account creation and modification procedures by the directors of CMS and Enterprise Systems and IT Security and Compliance.

7 Contacts

a) Questions regarding this procedure should be directed to: ITSecurity@calstatela.edu.

b) Questions regarding compliance, audits and auditing procedures should be directed to the University internal auditor at 323-343-5105.

c) Questions regarding the Student Administration system should be directed to the University registrar/director of Enrollment Services at 323-343-3940.

d) Questions regarding the Human Resources system should be directed to the assistant vice president for Human Resources Management at 323-343-3694.

e) Questions regarding the Financials system should be directed to the assistant vice president for Administration and Finance/Financial Services at 323-343-3615.

f) Questions regarding the Contributor Relations systems should be directed to the director of Advancement Services at 323-343-3072.

8 Related Documents

The following documents, forms and logs of the latest issue in effect shall apply to the extent specified herein.

ID/Control #	Title
ITS-1012-G	**User Guidelines for Oracle Access** http://www.calstatela.edu/its/itsecurity/guidelines This guideline helps users understand the different types of Oracle accounts, the process of obtaining one and compliance requirements for such an account.
ITS-1014-G	**User Guidelines for Student Administration Access** http://www.calstatela.edu/its/itsecurity/guidelines This guideline defines the criteria for authorized SA access and outlines the required steps to obtain and maintain an SA account.
ITS-2801	**Temporary PeopleSoft Administrative Access Request** http://www.calstatela.edu/its/forms/ITS-2801_TempPeopleSoftAdminAccessRequest.doc This form is used to request temporary access to the SA system.
ITS-6800	**New Student Administration Account Request Form** http://www.calstatela.edu/its/forms/get_account/ This form is used to request a new SA account.

ID/Control #	Title
ITS-6801	**Modification to Student Administration Account Request** http://www.calstatela.edu/its/forms/get_account/indexmodsa.htm This form is used to request a modification to or revocation of a user's current SA account.
ITS-6812	**Financials Information System Account Request Form** http://www.calstatela.edu/its/forms/get_account/indexfin.htm This form is used to request a new CFS account.
ITS-6813	**HR Information System Account Request Form** http://www.calstatela.edu/its/forms/get_account/indexhr.htm This form is used to request a new Human Resources account.
ITS-6814	**Contributor Relations Account Request Form** http://www.calstatela.edu/its/forms/get_account/indexcr.htm This form is used to request a new Contributor Relations account.
ITS-6817	**Modification to Human Resources Account Request** http://www.calstatela.edu/its/forms/get_account/indexmodcr.htm This form is used to request a modification to or revocation of a user's current Human Resources account.
ITS-6823	**Modification to Contributor Relations Account Request** http://www.calstatela.edu/its/forms/get_account/indexmodcr.htm 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** http://www.calstatela.edu/its/forms/get_account/indexmodcr.htm This form is used to request a modification to or revocation of a user's current Financials account.
ITS-8820	**Oracle Database Access Request** http://www.calstatela.edu/its/forms/ITS-8820_OracleAccessRequest.doc This form is used to apply for direct access to an Oracle database.
NA	**Chancellor's Office Certification of Annual Systems Access Review template** Available from the VP for ITS office, LIB PW 1070, 323-343-2600
NA	**Chancellor's Office Annual Review of PS Access Controls/Segregation of Duties Summary of Exceptions template** Available from the VP for ITS office, LIB PW 1070, 323-343-2600

ID/Control #	Title
NA	**Chancellor's Office Memorandum dated February 20, 2009 – Corrective Action for Audit Findings Reported in Conjunction with System-wide Financial and Single Audits for the Year Ended June 30, 2008** Available from the VP for ITS office, LIB PW 1070, 323-343-2600
NA	**Chancellor's Office Memorandum dated October 9, 2012 – Annual Access Control and Segregation of Duties Review.** Available from the VP for ITS office, LIB PW 1070, 323-343-2600
NA	**Chancellor's Office CSU Access Control and Segregation of Duties Procedures** Available from the VP for ITS office, LIB PW 1070, 323-343-2600