User Guidelines for Oracle Access	Guidelines No.	ITS-1012-G	Rev: B	Interim Release
	Owner:	IT Security and Compliance		
	Approved by:	Sheryl Okuno, Acting Director		
	Issued:	5/30/08	Effective:	5/30/08
				Page 1 of 8

1 Purpose

To protect confidential information, and to mitigate the high risk to the data, structural, and security integrity of the PeopleSoft applications, direct Oracle access is highly restricted and controlled. Oracle databases are limited to only those whose specific job duties require access when a task or troubleshooting cannot be performed using a normal PeopleSoft account. Direct Oracle database access is generally restricted to the campus Database Administrator(s) (DBA(s)) or remote CMS Data Administrator(s), depending on the system's physical location. However, functional support staff, Information Technology Services (ITS) technical support staff, consultants, and other users who cannot perform a job function through their regular PeopleSoft accounts occasionally may be granted direct Oracle access. DBAs and others who require direct Oracle access must apply for an Oracle account.

Access approval is based on necessity, not convenience. For example, access might be granted for technical staff to troubleshoot a problem, but would not be granted to run standard reports more quickly. Access levels differ depending upon users' job responsibilities and duties. Access and viewing privileges are controlled and limited to only defined portions of the Oracle database.

These guidelines are intended to help users understand the different types of Oracle accounts, the process for obtaining one, and compliance requirements for such an account.

2 Definitions

Functional Data Steward: The gatekeeper responsible for a specific functional area within the broader system. Examples: The Financial Aid functional area within the Student Administration system; or the Accounts Payable functional area within the Financials system.

Privileges: Security authorizations; permission to access an object

Roles: One or more privileges used to perform certain functions, such as, but not limited to, inserting, updating, deleting, and viewing data.

System Data Steward: The highest level of custodial review and data oversight from all functional areas within the respective steward's sphere of responsibility. This person approves or denies access to their respective systems through accounts.

3 Guidelines

3.1 Oracle Accounts and Usage

a) As a prerequisite for obtaining an Oracle 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).

b) Temporary Oracle access, if granted, is limited to a maximum of 90 days. Temporary accounts will be automatically locked at the close of business of the 90th day.

c) Each of the six different types of Oracle database user accounts have a different access level based upon job requirements and duties. In addition, there are also Oracle-delivered (default) accounts, which are locked (i.e., disabled). Oracle accounts and their access/privileges and purposes are listed in Table 1 below. The most common Oracle database privileges used at Cal State L.A are listed in Table 2 below.

Table 1. Oracle Accounts and Access Privileges

Account	Access/Privileges	Purpose/Restrictions
Oracle-Delivered	N/A	All are locked (disabled). No CSULA user may use this type of account.
Application Administrator/Database Owner	N/A	This account is created simultaneously when the database is created. It "owns" all application objects, but it is not actually employed as a user account (i.e., not used at all).
Database Administrator (DBA)	Full access, all privileges	Database installation, maintenance, and administration. Restricted to Campus/CMS DBAs and backup DBAs. Permanent access allowed.
Functional Support Staff	Access to transactional tables in a functional area	Use is based on job duties. Restricted to SELECT only access. Restricted to temporary access.
ITS Technical Support Staff	Temporary access to the production databases and/or permanent access to the development databases	Problem resolution by ITS staff. Restricted to ITS programmers. Restricted to SELECT only in PROD. Restricted READ/WRITE in DEVL and TEST databases. Restricted to temporary access
Consultants	Temporary access to databases	Perform functional or technical duties. Restricted to SELECT only in PROD. Restricted READ/WRITE in DEVL databases. Access based on contractual activities performed. Access duration must not exceed the consultant's contract duration. Restricted to temporary access.
Security Compliance	Permanent access to security audit tables	Conduct periodic reviews/audits of user access. Restricted to IT Security Management and Compliance staff. Permanent access allowed.

Table 2. Common Privileges Granted for CSULA Oracle Accounts

Privilege	Abbreviation	Use/Restrictions
ADMIN Option	SYSADM	SYSADM Option is the capability of re-granting the privilege to another user. Restricted to the campus/CMS DBA account only.
DELETE	DEL	Delete objects. Restricted to the campus/CMS DBA account only.
INSERT	INS	Inserts objects or data. Restricted to the campus/CMS DBA account only.
SELECT	SEL	Read only access. This is the only privilege granted to users other than the campus/CMS DBA in the Production and copy/clone of Production databases.
UPDATE	UPD	Read and write access. **Restricted to campus/CMS DBA accounts only.**

d) UPGRADE access is restricted to the campus/CMS DBA accounts only.

e) The Oracle systems at Cal State L.A. and data stewards responsible for them are listed in Table 3 below.

Table 3. System Data Stewards

System	System Data Steward
Contributor Relations	Assistant Vice President for University Development (Institutional Advancement)
Financials (CMS)	Associate Vice President, Administration and Finance/Financial Services (Administration and Finance)
Human Resources (CMS)	Director, Human Resources Management (Administration and Finance)
Student Administration (GET SA)	Director of Admissions and University Registrar (Student Affairs)

3.2 Oracle Account Creation

Access to Oracle databases is strictly limited and controlled. When individuals cannot perform troubleshooting or other tasks with their regular PeopleSoft account, they must request an Oracle account. Guidelines for the account request process are outlined in sections 3.2.1 (for a campus Oracle account) and 3.2.2 (for a CMS Oracle account) below.

3.2.1 Application for Campus Oracle Accounts

a) All Oracle users must renew their FERPA certificates of completion every two years by retaking the FERPA tutorial and test.

b) When requesting an Oracle account, a copy of the user's valid FERPA certificate of completion must be attached to the *Oracle Database Access Request* form (for employees) or the *Third Party Vendor/Consultant Oracle Database Access Request* form.

c) Direct Oracle access requires quarterly re-application and review.

3.2.2 Application for CMS Oracle Accounts

a) When requesting a CMS Oracle account, a copy of the user's valid FERPA certificate of completion must be attached to the *Oracle Database Access Request* form.

b) The user must complete the Chancellor's Office online *Request for Oracle Account* form, available on the CMS Web site at http://cms.calstate.edu/T3_Documents/CampusRequestForms/.

NOTE

Users who are restricted from accessing the CMS Web site should contact the CMS Project Director (see contacts in Section 5).

c) After completing the two forms referenced in steps a) and b), requestors must attach them together and forward both to the appropriate system data steward.

d) **No temporary access is granted for the CMS environment**.

3.2.3 Data Steward Responsibilities

a) Evaluate the request form(s). If this requestor's job title, employment responsibilities, and stated justification meet the criteria for allowing database access, continue to the next step. Otherwise, deny access by noting the reason for denial on the form, and then return a copy of the denied form(s) to the requestor. File the original request in your office.

b) Check the approved access privilege(s) you will grant this requestor (SELECT and/or UPDATE). Only DBAs are allowed UPDATE access.

c) Sign and date the form.

d) Forward the approved form to ITS (LIB PW 1070).

3.2.4 Information Technology Services (ITS) Responsibilities

a) Circulate the application to all on the ITS approval list, including the IT Security and Compliance director, the CMS Project director, and the VP ITS/CTO, for signatures and dates. If all the required individuals approve the request, continue to the next step. If not, enter the reason for denial on the form, return a copy of the form to the applicant, notify the data stewards, and file the original in the IT Security and Compliance director's office.

b) For campus-located systems, make a copy of the form and forward it to the campus DBA. Forward the original to the IT Security and Compliance director. For CMS remote systems, make two copies of the form and forward the original and one copy to the campus CMS Project director and one copy to the IT Security and Compliance director.

3.2.5 CMS Project Director Responsibilities

a) Electronically submit the approved *CMS Request for Oracle Account* form to the CMS Help Desk for action.

b) Attach a copy of the submitted form and all associated e-mail communications to the *Oracle Database Access Request* form and forward the packet to the Director, IT Security and Compliance, LIB PW 1070.

3.2.6 Campus or CMS DBA Responsibilities

a) Upon receiving the fully-approved application, create the account according to the instructions on the form.

b) Upon account creation, send an e-mail to the requestor with the following information:

- Username
- Initial password
- The **Are You Secure?** URL for password tips: http://www.calstatela.edu/its/itsecurity/tips/passwords.htm
- Instructions for changing the password
- Password expiration policy

c) File a copy of the form in your office.

3.3 Oracle User Account Modification

3.3.1 Transferred Users

a) When a user who is an employee is transferred to another group, department, or unit, or when a user's job responsibilities change, the user must reapply for an Oracle account (see Section 3.2) on the *Oracle Database Access Request* form. The "Modification" box must be checked.

b) When a user who is a third party vendor or consultant is transferred to another group, department, or unit, or if the third party's job responsibilities change, the third party's manager must notify the IT Security and Compliance director and the CMS Project director to revoke all access for that user. The CMS Project director must notify the Oracle DBA to revoke the account. Third parties must reapply for a new account if necessary.

3.3.2 Revoking Permanent Access

a) When an employee terminates employment with the University, Human Resources Management or University Auxiliary Services, Inc. (UAS) HR shall generate a separation notification and send it to department clearance personnel, including the ITS separation clerk. Upon receipt of the separation notice, the ITS separation clerk shall send this information via e-mail to a particular ITS distribution list that includes the Oracle DBA and the CMS Project director. If the separating employee has an Oracle account, the DBA shall revoke that user's access as of the date specified in the separation notification. The CMS Project director will notify the CMS Help Desk to revoke the user's account as of the date specified in the separation notice.

b) Access of third parties shall be terminated according to the date listed on the *Third Party Vendor/Consultant Oracle Database Access Request* form or when their services are terminated, whichever is sooner.

3.3.3 Revoking Access of an Abruptly Terminated Employee's or Third Party's Account

In the event an employee or third party is or will be abruptly terminated, Human Resources Management or University Auxiliary Services, Inc. (UAS) HR, or the third party's manager immediately shall give notice to the IT Security and Compliance director or the VP ITS/CTO by telephone or e-mail. Either the IT Security director or the VP ITS/CTO shall e-mail or otherwise send a memo to the CMS Project director and to the campus Oracle DBA(s) informing them to stand by for further instructions at a particular date and time. [Note: In the absence of the IT Security and Compliance director and the VP ITS/CTO, the memo will be e-mailed from the IT Security mailbox.] This memo shall **not** contain the employee's or third party's name. On the designated termination date and time, the IT Security and Compliance director or the VP ITS/CTO shall inform the CMS Project director and the campus Oracle DBA(s) of the employee's or third party's name and direct that all his/her Oracle accounts and other accounts be disabled immediately. The CMS Project director shall instruct the CMS Help Desk to revoke that user's accounts immediately.

3.3.4 Revoking Temporary Access

For all approved requests for temporary Oracle access, the IT Security and Compliance director shall create a new appointment in the Microsoft Outlook™ Calendar on the planned expiration date and schedule the DBAs and IT Security and Compliance personnel on it. When a reminder appears on the temporary access expiration date, the DBA shall lock the temporary account at the close of that business day. If an extension is required, the applicant must reapply, stating the reason for the extension in the justification.

IMPORTANT!

Hiring departments are responsible for immediately notifying IT Security and Compliance when a third party terminates employment prior to his/her contract or access expiration date.

3.4 Lockout after Failed Login Attempts

After a specified number of unsuccessful login attempts, an account will be locked for 30 minutes, after which the user can retry the login routine. If the login routine fails, the user must request a password reset (see section 3.5 below).

3.5 Password Reset

To request a password reset, the user must appear in person with his/her Golden Eagle Card (for employees) or photo ID (for third parties) at the ITS Help Desk (LIB PW Lobby) to request a password reset. The ITS Help Desk will verify the user's identity and employment prior to contacting the campus DBA. Since only a limited number of users have direct Oracle access and the DBA receives an application copy for all authorized users, the DBA must authenticate the user's rights and privileges before resetting the password.

3.6 Data Modification Process

a) Prior authorization from the responsible system data steward is required to modify data in a production environment. The requested SQL or procedure must be e-mailed to the DBA from the system data steward or designee. If the e-mail is sent from the designee, the data steward must be copied on it.

b) E-mail notifications concerning data modifications must be retained indefinitely by the DBA.

c) The system data steward must test and approve data modifications in a cloned database environment prior to the modifications being made in a production environment.

d) Production environment modifications must be scheduled to minimize system downtime and prevent conflict with ongoing production processes.

e) Modification logs or reports must be generated and maintained by the DBA for each production instance.

3.7 Periodic Reconciliation Process and Access Privilege Reviews

3.7.1 Data Modification Reviews

Data modification logs and reports may be requested without prior notice no less than once each quarter by IT Security and Compliance for the purpose of reconciling approved requests with the actual modifications made. Any items that cannot be reconciled with an authorized change must be investigated by IT Security and Compliance.

3.7.2 Access Privilege Reviews

No less than once each quarter, the IT Security and Compliance staff will conduct a review to ensure that the access and privileges of authorized users have been appropriately assigned. As part of this review, the list of Oracle user accounts will be compared with Human Resources Management personnel data to ensure that only current employees have access to the database. Consultant user accounts will be verified with the hiring department to validate that a current contract is still in place.

3.8 Reporting Security Breaches and Violations

a) 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 Information Technology Services and CTO
Phone: 323-343-2600
ITSecurity@calstatela.edu

Director of IT Security and Compliance
Phone: 323-343-2600
ITSecurity@calstatela.edu

b) The Vice President for Information Technology Services and CTO, as well as the Director of IT Security and Compliance, are responsible for notifying University Counsel within 30 minutes of discovery and providing periodic updates as required.

c) All security breaches and violations shall be investigated forthwith, followed up with a report containing analysis of the matter and recommendations for action.

d) The DBA and the Director of IT Infrastructure are responsible for addressing all campus action items. The campus CMS Project Director is responsible for addressing all CMS action items.

e) The final report(s) shall be filed with the Director of IT Security and Compliance.

4 Terms, Conditions, and Sanctions

a) All individuals with authorized account access must comply with the state and federal laws, including the Family Educational Rights and Privacy Act (FERPA) and California Government Code section 8314, and University policies that govern access to, and use of, information contained in employee, applicant, and student records, whether these records are printed or electronic. 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.

b) A violation of information security precautions may be a crime and may result in any legal and disciplinary actions that apply, including criminal prosecution.

c) A violation may furnish the basis for disciplinary actions as set forth by statute, including but not limited to Education Code section 89535, up to and including dismissal.

d) Illegal use of data, computers, programs, systems, networks, or supporting documentation is a violation of Penal Code Sections 502 and 502.01 and is punishable by fine and/or imprisonment.

e) Any third party in violation of these guidelines or any law will lose all access privileges, and the third party's company will be disqualified from Cal State L.A. bids, purchase orders, contracts, and awards for a period of two (2) years.

5 Contacts

a) To report a security breach or violation, immediately notify the Director of IT Security and Compliance and/or the Vice President for ITS and CTO at to ITSecurity@calstatela.edu.

b) To report problems accessing the Oracle Database Access Request form, contact the ITS Help Desk at (323) 343-6170 or LIB PW Lobby.

c) To report problems accessing the CMS Request for Oracle Account form, contact the CMS Project director at (323) 343-2600.

d) Questions regarding these guidelines should be addressed to ITSecurity@calstatela.edu.

6 Related Documents

ID/Control #	Title
ITS-8820	**Oracle Database Access Request** Form used to request direct access to an Oracle database. http://www.calstatela.edu/its/forms
N/A	**CMS Request for Oracle Account** Chancellor's Office form used to apply for CMS Oracle Accounts http://cms.calstate.edu/T3_Documents/CampusRequestForms/