Financial Management System (FMS)
User Access Control

Lawrence Berkeley National Laboratory | **Financial Policies and Procedures** | **Part I**

Originally issued:	December 17, 2007
Effective Date:	February 19, 2008
Revision Number:	1
Scheduled review date:	December 17, 2008 (every year)
Primary contact:	Manager, Business Systems Analysis

Summary

The Office of the CFO (OCFO) is responsible for the secure stewardship and control of the system throughout its lifecycle. The objective of this policy is to define control procedures that restrict system access to authorized Financial Management System (FMS) users, and to limit user privileges based on business need.

Policy

The OCFO is responsible for managing FMS user access and privileges. This includes setting up user accounts as well as activating, modifying, reviewing, and disabling those accounts.

The OCFO employs this policy and a variety of security enforcement mechanisms to control user access to FMS. Consistent with RPM §9.01, Paragraph E, *Information and Computer Security Responsibilities*, these controls are established to ensure that data in FMS is sufficiently protected from unauthorized use, alteration, and manipulation, and that users, data owners and system owners take appropriate precautions to secure FMS and the data contained therein.

Division Managers and Supervisors are responsible for communicating changes in employee job responsibility and/or employment status to the Business Systems Manager. When an employee is terminated the Termination Notification System (TNS) automatically locks the user's FMS account preventing further system access.

The OCFO conducts FMS security reviews at least annually to ensure that users' access and privileges are appropriate and consistent with their current job responsibilities.

Procedures

Roles & Responsibilities

Business Systems Analysis Manager or Designee

- Manages FMS user access controls consistent with this policy.
- Grants access to FMS based on manager/supervisor authorization.
- Supports system module owners in defining and documenting requirements for basic and enhanced FMS user access and privileges. Where changes are required, communicates functional requirements to Information Technology Institutional Systems (ITIS).
- At least once a year, coordinates and documents the functional review and confirmation of FMS user access and privileges assigned to users.
- Establishes the time limit for automatic application time-outs and communicates these parameters to IT.
- Manages use of anonymous accounts (see glossary).

OCFO System Module Owner

- Working with the Manager of Business Systems Analysis or designee, defines requirements for user access and privileges. For user roles that provide enhanced FMS user access the system module owner establishes access criteria such as completion of specific skills training and appropriate job titles.
- Identifies exclusive roles requiring separation of functional duties/responsibilities. Working with the Manager of Business Systems Analysis or designee ensures that no user has access to incompatible exclusive roles.
- Reviews and approves requests for enhanced FMS user access due to changes in a user's job responsibility or organization. Verifies pre-conditions are met and that the intended system usage is appropriate.
- Submits approved system access and privilege changes via email to Business Systems Analysis Manager or designee.
- Where appropriate, manages organization-level user access to modules.
- Periodically reviews and, as necessary, requests changes to basic and enhanced system access and privileges consistent with business requirements.
- At least once a year, reviews and confirms FMS user access and privileges.

Supervisors of FMS Users (including employees and/or guests)

- Requests enhanced FMS user access via email from the System Module Owner, consistent with user job responsibilities. Ensures that access pre-conditions and criteria (such as completion of specific skills training) are completed by the new user.
- If an FMS user's job responsibility or organization changes, assesses whether a change to their FMS access is required. If so, requests an FMS access change via email from the System Module Owner.
- Requests changes to enhanced FMS access from the System Module Owner whenever changes to an FMS user's job responsibilities require modifications to their FMS access. See wiki for request access: https://www.lbl.gov/wiki/bin/view/Main/SysAccess

ITIS (Information Technology Institutional Systems)

- Based on functional specifications and consistent with this policy, establishes, monitors and maintains system parameters and controls in support of the requested system access and privileges.
- Supports the annual (or more frequent) review and confirmation of assigned user access and privileges.
- Maintains the time limit for automatic application time-outs based on input from Business Systems Analysis Manager.

Authority

- LBNL Regulations and Procedures Manual Section §9.01, Computing and Communications.
- OCFO Business System Ownership policy

Contacts

- Manager, OCFO Business Systems Analysis

Glossary

- ***Anonymous accounts:*** Established to run background processes and/or to test and maintain system capabilities.
- ***Enhanced FMS User Access:*** Additional access to FMS capabilities beyond the basic access provided to all new employees and guests typically providing read/write permissions.

- ***Financial Management System (FMS)***: FMS is comprised of the following components: General Ledger, Project Cost, Commitment Control Ledger, Accounts Payable, Billing, Accounts Receivable, RAPID Grants Management, eProcurement, eBuy, Funding Database, and Field Budget Submission System (FBSs). Access to all of these components is managed using a common PeopleSoft access security panel.

- ***System Module Owner***: Functional manager with assigned responsibility for an FMS system component consistent with the OCFO Business System Ownership policy.

- ***User***: Individual employee, guest or system process authorized to access an information system.