Financial Management System (FMS) User Access Control

BRIEF

Policy Summary

Berkeley Lab's Office of the Chief Financial Officer (OCFO) is responsible for managing the secure stewardship and control of its business and financial systems. This includes maintaining clearly defined roles and permissions, setting up and managing user accounts, and ensuring that users' access privileges and assigned roles are approved and consistent with business needs.

Who Should Read This Policy

Any Berkeley Lab employee responsible for managing user access for Laboratory business and financial systems

To Read the Full Policy, Go To:

The POLICY tab on this wiki page

Contact Information

Deputy Chief Financial Officer or
OCFO Business Systems Analysis (BSA) Manager

POLICY

A. Purpose

This document defines the policy and procedures for managing Office of the Chief Financial Officer (OCFO) business and financial system user access controls, which includes roles and permissions, user accounts, and access privileges that meet approved criteria and are consistent with business needs.

B. Persons Affected

Any Lawrence Berkeley National Laboratory (Berkeley Lab) employee responsible for managing user access for Laboratory business and financial systems

C. Exceptions

None

D. Policy Statement

OCFO is responsible for managing the secure stewardship and control of its business and financial systems. This includes maintaining clearly...
defined roles and permissions, setting up and managing user accounts, and ensuring that users' access privileges and assigned roles are approved and consistent with business need.

OCFO employs this policy and a variety of security-enforcement mechanisms for controlling system user access. Consistent with the Berkeley Lab Requirements and Policies Manual (RPM) Security for Information Technology policy, these controls ensure that data resident in systems are sufficiently protected from unauthorized use, alteration, and manipulation; and that users, data owners, and system owners take appropriate precautions to secure business and financial systems and the data contained therein.

Division managers and supervisors are responsible for communicating changes in employee job responsibility and/or employment status to the OCFO System Module Owner, Business Systems Manager, or designee. For some OCFO systems, such as the PeopleSoft Financial Management System, Berkeley Lab's Termination Notification System (TNS) automatically locks the user's account, preventing further system access when an employee is terminated.

OCFO employs a risk-based approach to conducting regular reviews and validations of users' system access.

E. Roles and Responsibilities

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibility</th>
</tr>
</thead>
</table>
| Business Systems Analysis Manager or Designee | • Manages the OCFO business and financial system user access program consistent with this policy  
• Ensures that changes to a user's access and privileges are authorized by the user's manager or supervisor  
• Supports system module owners in defining and documenting requirements for basic and enhanced user access and privileges. Where changes are required, communicates functional requirements to the IT Business Systems unit.  
• Conducts and/or coordinates regular reviews of user access and privileges as defined in the attached Risk Based User Access Program  
• Establishes the time limit for automatic application time-outs and communicates these parameters to IT  
• Manages the use of anonymous accounts       |
| OCFO System Module Owner or Designee      | • Working with the Manager of Business Systems Analysis or designee, defines requirements for user access and privileges related to a specific module. For user roles that provide enhanced user access, the System Module Owner establishes access criteria such as completion of specific skills training, appropriate job titles, or other criteria consistent with business need.  
• Identifies roles that are incompatible due to potential conflict of interest requiring separation of functional duties/ responsibilities. Working with the Manager of Business Systems Analysis or designee, ensures that no user has access to multiple roles that, when assigned to the same user, create a potential for conflicts of interest.  
• Reviews and approves requests for enhanced user access. Verifies pre-conditions are met and that the intended system usage is appropriate.  
• Submits approved system access and privilege changes via e-mail to Business Systems Analysis Manager or designee  
• Where applicable, manages user access to division-specific (i.e., row-level) information  
• Periodically reviews and, as necessary, requests changes to basic and enhanced system access and privileges consistent with business requirements  
• Participates in regular user access reviews to help confirm user access and privileges       |
| Supervisors of System Users (including employees and/or affiliates) | • Request enhanced user access via e-mail from the System Module Owner (or designee), consistent with business need. Ensure that access pre-conditions and criteria (such as completion of specific skills training) are completed by the new user.  
• If a user's assigned job responsibility, organization, or other condition changes, assess whether a change to the user's systems access or privilege level is required. If so, request this change via e-mail from the System Module Owner (or designee).       |
| ITBS (IT Division Business 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 regular access reviews and confirms access and privileges assigned to ITBS staff  
• Maintains the time limit for automatic application time-outs based on input from Business Systems Analysis Manager       |

F. Definitions/Acronyms

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous Accounts</td>
<td>System accounts established to run background processes and/or to test and maintain system capabilities</td>
</tr>
<tr>
<td>Enhanced User Access</td>
<td>Additional access to system capabilities that provide read/write permissions and/or read access to sensitive information</td>
</tr>
<tr>
<td>System Module Owner</td>
<td>Functional manager with assigned responsibility for a system component consistent with the OCFO Business System Ownership policy</td>
</tr>
</tbody>
</table>
User

Individual employee, affiliate, or system process authorized to access an information system

G. Recordkeeping Requirements

None

H. Implementing Documents

<table>
<thead>
<tr>
<th>Document Number</th>
<th>Title</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.04.003.001</td>
<td>Risk Based Review — Categories, Criteria and Review Cycle</td>
<td>Procedure</td>
</tr>
</tbody>
</table>

I. Contact Information

Deputy Chief Financial Officer or OCFO Business Systems Analysis (BSA) Manager

J. Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Revision</th>
<th>By whom</th>
<th>Revision Description</th>
<th>Section(s) affected</th>
<th>Change Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>3/25/2013</td>
<td>1.1</td>
<td>Axthelm</td>
<td>Review completed 12/17/2012, no changes</td>
<td>Pub &amp; next review dates</td>
<td>Minor</td>
</tr>
<tr>
<td>1/2/2012</td>
<td>1</td>
<td>Axthelm</td>
<td>Reformat for wiki</td>
<td>All</td>
<td>Minor</td>
</tr>
</tbody>
</table>

Document Information

**DOCUMENT INFORMATION**

- **Title:** Financial Management System (FMS) User Access Control
- **Document number:** 11.04.003.000
- **Revision number:** 1.1
- **Publication date:** 3/25/2013
- **Effective date:** 12/7/2011
- **Next review date:** 12/17/2013
- **Policy Area:** Financial Business Systems
- **RPM Section (home):** Financial Management
- **RPM Section (cross-reference):** Section 11.49
- **Functional Division:** OCFO
- **Prior reference information (optional):** RPM Section 11.49

Source Requirements Documents

None

Other Driving Requirements

<table>
<thead>
<tr>
<th>Document Number</th>
<th>Title</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.04.002.000</td>
<td>Business System Ownership</td>
<td>Policy</td>
</tr>
<tr>
<td>10.01.002.000</td>
<td>Security for Information Technology</td>
<td>Policy</td>
</tr>
</tbody>
</table>

Implementing Documents

Lawrence Berkeley National Laboratory. The official or current version is located in the online LBNL Requirements and Policies Manual. Printed or exported versions are not official. Users are responsible for working with the latest approved revision.
<table>
<thead>
<tr>
<th>Document Number</th>
<th>Title</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.04.003.001</td>
<td>Risk Based Review — Categories, Criteria and Review Cycle</td>
<td>Procedure</td>
</tr>
</tbody>
</table>