Lifecycle Management for Information, Hardware, Software, and Services

BRIEF

Policy Summary

This policy establishes line management and individual responsibility for lifecycle management of Laboratory Information and Laboratory Information Technology (IT) assets at Berkeley Lab. This policy complements other policies on aspects of lifecycle management, including security and information controls. This policy describes responsibilities and requirements for lifecycle management of Berkeley Lab's:

- Information
- Institutional (centrally provided) services
- Hardware, software, and services, including acquisition restrictions
- Software with special considerations, including:
  - Safety Software
  - Software with physical interfaces
  - Hardware and software assets, and services, including acquisition restrictions

Who Should Read This Policy

Employees and affiliates who use or manage Laboratory Information or IT; employees and affiliates who acquire, develop, or manage hardware, software, or services

To Read the Full Policy, Go To:

The POLICY tab on this wiki page

Contact Information

Information Technology Policy Manager
Information Technology Division
itpolicy@lbl.gov

Policy

A. Purpose
This policy establishes lifecycle management for information, hardware, software, and services to promote the efficient management of Laboratory Information and IT, while facilitating the scientific mission of Lawrence Berkeley National Lab (Berkeley Lab).

B. Persons Affected

Employees and affiliates who use or manage Laboratory Information or IT; employees and affiliates who acquire, develop, or manage hardware, software, or services.

C. Exceptions

Not applicable

D. Policy Statement

D.1 Employee Responsibilities

Everyone is responsible for lifecycle management. Lifecycle management is a line-management function at Berkeley Lab. Laboratory employees and affiliates are responsible for the lifecycle management of Laboratory Information and Laboratory IT that they use or manage. Lifecycle management includes:

- Planning and project management, including disaster and continuity planning
- Security throughout the lifecycle
- Acquisition, development, and implementation
- Management, operations, backups, and maintenance and
- Disposal or retirement

D.2 Institutional Services

For both security and efficiency reasons, the Chief Information Officer identifies select services as Institutional Services. Only the responsible office or its designee may provide Institutional Services.

D.3 OperationsDivisions

Operations divisions may not acquire hardware, software, or services to support operation-level activities without coordination with and approval from the IT Division.

D.4 Researchers and Research Divisions

In general, researchers and their line management are in the best position to identify hardware, software, and service needs, excluding Institutional Services. When identifying needs, researchers should use a cost-benefit approach to evaluate commercial, open source, custom, or other existing solutions. This section provides additional requirements or policy to promote responsible stewardship.

1. General Requirements for Software Development
   a. Lifecycle Management. Researchers should consider what components of lifecycle management, including quality assurance, are appropriate to the risks and uses of their software. In general, the peer review process constitutes adequate quality assurance for software developed for research purposes.
   b. Licensing. Researchers should consider licensing options early in their project and contact the Innovation and Partnerships Office for assistance.
   c. Disclosure Requirement. Under certain circumstances, researchers must submit software developed in the course of their work at Berkeley Lab per requirements of the Software Disclosure and Distribution policy.

2. Software and Service Acquisition
   a. Acquisition. If unavailable through Laboratory venues (e.g., software.lbl.gov and ebuy.lbl.gov), researchers may acquire software via standard procurement procedures. Researchers may acquire IT services provided that the services meet security requirements as appropriate. Guidance: Cloud Services - Things to Consider.
      i. For cloud providers, researchers should assess the risks and identify any controls to mitigate those risks. Guidance: Cloud Services - Things to Consider.
      ii. Researchers must contact Cyber Security to discuss appropriate controls if a software or service:
         1. Has deep, persistent connections to institutional business systems or
         2. Has a Berkeley Lab domain name and is highly visible to the outside world such that compromise or failure would be newsworthy or
         3. Processes sensitive data such as Personally Identifiable Information (PII) or institutional financial or safety data with special integrity and availability requirements
b. **Licensing Agreements.** Berkeley Lab permits licensing agreements in which the user accepts the agreement by clicking or opening the package. A Procurement representative must sign licensing agreements that require signatures.

3. **Hardware Acquisition.** In support of our mission, Berkeley Lab encourages system choice to support the diverse needs of researchers. Divisions and groups may set hardware standards or leave hardware decisions to the discretion of the principal investigator or end user. Standards and decisions should be based on managing lifecycle costs in support of effectively achieving research missions.

**D.5 Safety Software and Software with Physical Interfaces**

During the course of research or operations, employees and affiliates may be involved with the development, maintenance, management, or use of Safety Software or software with physical interfaces. Employees and affiliates must adhere to the following requirements.

1. **Safety Software.** Safety Software is software whose degradation can have a direct effect on human safety (see full definition in Section F, below). Safety Software at Berkeley Lab must be appropriately approved, controlled, and tested.
   a. **Approval and Inventory.** Software that meets the definition of Safety Software must be reported to the Environment/Health/Safety (EHS) Division for approval. EHS must approve the development of safety software in coordination with the Information Technology Division. The Office of Contractor Assurance maintains the Safety Software Inventory, and the organization that owns or uses the software updates the inventory.
   b. **Safety Software Quality Assurance Requirements.** Anyone involved in the development, maintenance, management, or use of software on the Safety Software Inventory must adhere to the Safety Software Quality Assurance Requirements.
   c. Where software is part of a safety chain, but where a nonsoftware control protects human safety from software degradation, management may adopt a subset of the Safety Software Quality Assurance Requirements at its discretion.

2. **Software with Physical Interfaces.** Software used to monitor or interact with the physical world presents additional risks. This software usually includes programmable logic controllers (PLC) and supervisory control and data acquisition systems (SCADA). Even where this software does not rise to the level of Safety Software, it still merits deliberate controls and testing. Anyone involved in the development, maintenance, management, or use of software with physical interfaces should conduct a risk analysis and identify appropriate controls. When conducting the risk analysis, consider the whole system, including both software and nonsoftware components. Specific risks to consider include cyber security, data integrity, and damage to equipment.

**D.6 Open Source Software**

The Laboratory encourages the use of open source software and contributing to open source projects provided that contributions are within the terms associated with the funding for the work.

1. **Cyber Security.** Open source software may have cyber security benefits as multiple individuals view the code. However, use caution, especially with smaller projects. Download the software from a reputable source and, when available, use tools to check the integrity of the code (e.g., checksums).

2. **Licensing.** Open source software is typically released under a license that creates a legal obligation between the copyright holder and Berkeley Lab. Users must review and adhere to the licensing restrictions, especially when modifying or including the code within other software.

**D.7 Information Technology Division**

The Information Technology Division is responsible for developing and maintaining a graded approach to IT lifecycle management, from conception to retirement. All IT-managed services (including institutional), hardware, software, and outsourced services must adhere to the IT lifecycle management approach, which incorporates grades based on risk to physical safety as well as privacy.

**E. Roles and Responsibilities**

Employees and affiliates are responsible for adhering to this policy.

**F. Definitions/Acronyms**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Safety Software includes the following:

1. Safety System Software. Software for a nuclear facility that performs a safety function as part of a structure, system, or component (SSC) and is cited in either (a) a DOE-approved documented safety analysis or (b) an approved hazard analysis per DOE P 450.4, Safety Management System Policy, dated 10-15-96 (or latest version) and 48 CFR 970-5223.1.
2. Safety and Hazard Analysis Software and Design Software. Software used to classify, design, or analyze nuclear facilities. This software is not part of an SSC but helps to ensure the proper accident or hazards analysis of nuclear facilities or an SSC that performs a safety function.
3. Safety Management and Administrative Controls Software. Software that performs a hazard control function in support of nuclear facility or radiological safety management programs or technical safety requirements or other software that performs a control function necessary to provide adequate protection from nuclear facility or radiological hazards. This software supports eliminating, limiting, or mitigating nuclear hazards to workers, the public, or the environment as addressed in 10 CFR Parts 830 and 835, the DEAR Integrated Safety Management System clause, and 48 CFR 970-5223.1.

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>10.01.003.001</td>
<td>Institutional Services</td>
<td>List</td>
</tr>
<tr>
<td>10.01.003.002</td>
<td>Safety Software Inventory</td>
<td>List</td>
</tr>
<tr>
<td>10.01.003.004</td>
<td>Safety Software Quality Assurance Requirements</td>
<td>Standard</td>
</tr>
</tbody>
</table>

I. Contact Information

Information Technology Policy Manager
Information Technology Division
itpolicy@lbl.gov

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>1/2/2012</td>
<td>0</td>
<td>J. Bonaguro</td>
<td>Rewrite for wiki (brief)</td>
<td>All</td>
<td>Minor</td>
</tr>
<tr>
<td>11/28/2012</td>
<td>1</td>
<td>J. Bonaguro</td>
<td>Rewrite for wiki (policy)</td>
<td>All</td>
<td>Minor</td>
</tr>
<tr>
<td>3/22/2017</td>
<td>1.1</td>
<td>S. Lau</td>
<td>Technical edits</td>
<td>All</td>
<td>Minor</td>
</tr>
</tbody>
</table>

Document Information

DOCUMENT INFORMATION

<table>
<thead>
<tr>
<th>Title:</th>
<th>Lifecycle Management for Information, Hardware, Software, and Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Document number</td>
<td>10.01.003.000</td>
</tr>
<tr>
<td>Revision number</td>
<td>1.1</td>
</tr>
<tr>
<td>Publication date</td>
<td>3/22/2017</td>
</tr>
<tr>
<td>Effective date</td>
<td>9/20/1996</td>
</tr>
<tr>
<td>Next review date</td>
<td>3/22/2020</td>
</tr>
<tr>
<td>Policy Area</td>
<td>Information Technology</td>
</tr>
<tr>
<td>RPM Section (home)</td>
<td>Information Management</td>
</tr>
<tr>
<td>RPM Section (cross-reference)</td>
<td>Section 9.02(E)</td>
</tr>
</tbody>
</table>
**Source Requirements Documents**

- DOE O 200.1A, *Information Technology Management, CRD*
- DOE O 414.1C, *Quality Assurance, Attachment 1, CRD*
- DOE O 205.1B, *Department of Energy Cyber Security Program, CRD*
- DOE Office of Science *Program Cyber Security Plan, June 2010*
- Berkeley Lab Senior Management requirement

**Implementing Documents**

<table>
<thead>
<tr>
<th>Document Number</th>
<th>Title</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.01.003.001</td>
<td>Institutional Services</td>
<td>List</td>
</tr>
<tr>
<td>10.01.003.002</td>
<td>Safety Software Inventory</td>
<td>List</td>
</tr>
<tr>
<td>10.01.003.004</td>
<td>Safety Software Quality Assurance Requirements</td>
<td>Standard</td>
</tr>
</tbody>
</table>