Jacobsen Declaration
Exhibit F

§9.01
Computing and Communications

Responsible Manager

Rev. 08/05

A. INTRODUCTION

This section contains basic Ernest Orlando Lawrence Berkeley National Laboratory policy governing computing and communications. Operational procedures and guidelines may be found in RPM §9.02 (*Operational Procedures for Computing and Communications*).

B. AUTHORIZED USE OF FACILITIES

All usage of Laboratory computing and communications facilities must be limited to authorized use. Authorized use is limited to official Laboratory business except as otherwise noted in this manual.

C. AUTHORIZED USE OF INFORMATION RESOURCES

1. Purpose and Scope

The purpose of this policy is to set forth requirements and restrictions on the use of Laboratory information resources. All Laboratory information resources are government property and, as such, are subject to the requirements in the DOE/LBNL Contract, Laboratory policy, and federal and state laws on the proper use, protection, accountability, and disposition of government property. See also RPM §§2.18(C)(1) (*Use of Laboratory Equipment, Supplies, and Services*), 6.02(A) (*General*), 9.02(D)(10) (*Information Security Guidelines*).

These contract provisions, Laboratory policies, and laws apply to all data-communication and telecommunication facilities, equipment, and services located on or off site, including, but not limited to, personal computers, workstations, networking services, mainframes, minicomputers, associated peripherals and software, electronic mail, telephones, voicemail, and faxes.

Questions regarding this policy should be addressed to individual supervisors or the Computer Protection Program Manager. NERSC and ESNet users should also refer to the usage policies at http://www.nersc.gov/nusers/policy/ and http://www.es.net/hypertext/esnet-aup.html, respectively.

2. Applicability

This policy applies to all users of Laboratory information resources, including, but not limited to, employees, contract labor workers, students, visitors, and guests.

3. Policy

a. Scope of Authorized Use

Laboratory information resources are funded by the United States government for the purpose of supporting the Laboratory's scientific, programmatic, and administrative activities. These resources are made available to users for the purpose of conducting the Laboratory's official business. For definition of "official use," see Paragraph (C)(4)(a), below.

"Incidental personal use," as defined in Paragraph (C)(4)(b), below, is allowed with the explicit understanding that no message sent or received is private and that such messages may be reviewed or retrieved by authorized Laboratory personnel in furtherance of their official duties. Such authorized personnel will be appointed under procedures implementing this information resources policy.

Note that special restrictions apply to the monitoring or recording of telephone conversations. With certain limited exceptions, it is illegal to monitor or record telephone conversations without the consent of all participants. For limitations on the personal use of Laboratory telephones, see RPM §9.02(A)(2)(e)

(*Personal Calls*).

User IDs, passwords, encryption, access codes, and all other such devices, present and future, are provided for the purpose of limiting access to the system so as to maintain security of information systems and the information they contain for the official business purposes for which they are dedicated, not for the purpose of providing confidentiality for personal messages. Users are responsible for adhering to appropriate access procedures and may be held accountable for failing to follow such procedures or for gaining access to systems, data, or information beyond their authorization; e.g., users should not read or browse through another's e-mail or data except in emergency circumstances.

b. Notice to Users

To ensure that users are aware of this policy and to comply with DOE mandate, the following banner will appear each time a user accesses any Laboratory computer system:

NOTICE TO USERS

> Lawrence Berkeley National Laboratory operates this computer system under a contract with the U.S. Department of Energy. It is the property of the United States Government and is for authorized use only. The use of this system may be monitored for computer security purposes. Any unauthorized access to this system is prohibited and is subject to criminal and civil penalties under Federal Laws including but not limited to Public Laws 83-703 and 99-474. Each time you use this system (from here, from home, or on your personal laptop connected to an LBNL system), you consent to such interception, auditing, and related activity by authorizing personnel; further, LBNL may detain, access, and copy files from a non-LBNL computer when there is reason to believe misuse has occurred.
>
> - LBNL Computer Protection Emergency phone number: 486-7770
> - LBNL Security Web page: http://www.lbl.gov/security/
> - LBNL Backup Services: http://www.lbl.gov/ITSD/CIS/Services/backups.html

4. Definitions

a. Official Use

"Official use" for the purpose of this policy is a use that supports or is related to the conduct of Laboratory business. In addition to activities obviously required for one's job (e.g., scientific research, engineering computations, sharing technical information for review, comment and information exchange, technical collaboration or participation in professional organizations as part of one's research activities, office correspondence, and administrative functions), official use includes activities such as the following:

- Professional development and educational activities related to the user's Laboratory work assignment;

- Incidental perusal of information (e.g., news groups) for educational or professional development related to the user's work assignment;
- Laboratory-approved community relations and support activities; and
- Use of such resources on behalf of national, state, and local committees or task forces when the Laboratory has permitted work time to be used for these purposes.

b. Incidental Personal Use

"Incidental personal use" is allowed as long as it is consistent with this policy and all implementing policies and procedures and does not:

- Directly or indirectly interfere with Laboratory operation of such resources;
- Burden the Laboratory with noticeable incremental cost;
- Interfere with the user's employment or other obligations to the Laboratory; or
- Constitute an "unacceptable use," as defined in Paragraph (C)(4)(c), below.

Users who elect to engage in such incidental personal use should do so, as noted in Paragraph (C)(3)(a), above, with no expectation of personal privacy concerning the messages they compose, transmit, or receive.

c. Unacceptable Use

Activities that constitute "unacceptable use" of Laboratory information resources include, but are not limited to, the following:

- Use of such resources for personal gain, lobbying, or unlawful activities such as fraud, embezzlement, theft, or gambling;
- Use of resources for unlawful discrimination, harassment, or retaliation;
- Unauthorized entry into or tampering with computers, networks, or other information resources;
- Use of resources in a manner intended to, or likely to result in, damage to any system, database, or intended official use (e.g., distributing viruses);
- Misusing or forging e-mail or tampering or gaining unauthorized access to the Laboratory's e-mail system;

- Use of e-mail to give the impression that the user is representing, giving opinions, or otherwise making statements on behalf of the Laboratory unless appropriately authorized (explicitly or implicitly) to do so;
- Use of resources to create, download, view, store, copy, or transmit sexually explicit materials or images;
- Use of resources in connection with conduct or activities prohibited by Laboratory policy (e.g., fabrication, falsification, or plagiarism in proposing, conducting, or reporting research; unauthorized disclosure of Laboratory proprietary information) or use in violation of applicable copyright or patent laws;
- Unauthorized or unlawful monitoring or recording of telephone conversations;
- Unauthorized use of resources on behalf of outside organizations or any use that conflicts with or is inconsistent with Laboratory information resources policies or procedures;
- Use of resources to store, manipulate, or remotely access any national security information, including, but not limited to, classified information, unclassified controlled nuclear information (UCNI), and naval nuclear propulsion information (NNPI); or
- Any use that violates applicable federal or state laws or regulations.

5. Sanctions for Misuse of Information Resources

Any use of Laboratory information resources in violation of this policy may result in one or more of the following sanctions:

- Restriction of access to such resources
- Disciplinary action, up to and including dismissal
- Loss of site-access privileges for contract labor workers, students, visitors, and guests
- Referral to federal or state law enforcement authorities for appropriate action, including criminal prosecution, if such use violates the law

D. COMMUNICATIONS EQUIPMENT, RESOURCES, AND SERVICES

All requests for communications and networking resources or services must be processed through the Networking and Telecommunications Department. Unauthorized personnel may not install, remove, or modify equipment belonging to or managed by this department. Unauthorized equipment may not be installed or attached to network or telecommunications systems.

E. OPERATIONAL MANAGEMENT

Laboratory voice telephone, cellular telephone, data-switching, networking, and teleconferencing systems (except for public address and radio communications systems; see below) are managed by the Networking and Telecommunications Department (NTD) of the Computing Sciences Directorate. Laboratory policies and DOE orders pertaining to the design, acquisition, management, and operation of all types of communications resources are administered by NTD. Reviews of DOE orders pertaining to voice, data, and networking resources and to all associated interactions with DOE and DOE/OAK are conducted through the Computing Sciences Directorate.

F. PUBLIC ADDRESS SYSTEM

Use of the public address system is reserved at all times for emergencies, health and safety matters, or announcements of interest to the entire Laboratory population. Prior approval by the Associate Laboratory Director for Operations is required for any announcement not necessitated by an emergency, health, or safety situation.

G. SECURITY

The Laboratory's computer systems and all information contained in these systems must be protected from improper use, alteration, manipulation, or unauthorized disclosure. Failure to observe proper computer and network security practices will result in disciplinary action, including possible termination.

1. Security Responsibilities

a. The Laboratory Chief Information Officer (CIO) is responsible for overall cyber security as described in the Cyber Security Program Plan (CSPP).

b. Computer system managers are responsible for implementing the CSPP by providing security measures appropriate to their systems and for informing their users of these security measures. System managers are also responsible for informing their users of any usage restrictions on licensed or proprietary software.

c. Data and application owners are responsible for taking suitable precautions to ensure an appropriate level of physical and electronic security.

d. Users are responsible for all activity carried on through their user ID, whether authorized or not.

2. Confidentiality

It is Laboratory policy that all computer files be accessible only by the person responsible for those files unless that person has explicitly authorized others to access them. Access may be granted to the person's supervisor or manager if it is necessary for Laboratory purposes. This policy applies regardless of the level of access protection assigned to a particular file.

Chapter 9 Contents | **RPM Contents** | **Home** | **Search the RPM**