

Lawrence Berkeley National Laboratory Computer Protection Agreement

All employees, guests, and subcontractors share in the responsibility to protect the Laboratory's information assets and resources and to use LBNL computer resources in a responsible manner. The following security rules are highlights from the formal LBNL computer security policy as enunciated in the applicable Policy Procedure Memos and in the Regulations and Procedures Manual. These rules apply to all LBNL computer users, regardless of the size or location of the computer system involved.

1. As passwords are the key to computer access security, they must not be:
 - 1• Shared with anyone not authorized to access the system in question.
 - 2• Kept in a "public" place where any other person has access or accidental disclosure would be likely.
2. Use LBNL computers for authorized purposes only.
3. Do not use or make copies of unauthorized software. Unauthorized software includes unlicensed commercial software and software that can be used to assist in gaining unauthorized access to computer systems.
4. Do not load or use any software from a source not known to be reliable. Unmoderated public bulletin boards are not reliable sources.
5. Observe all system-specific computer security policies and procedures established by the system manager of any system you use.
6. Do not attempt any unauthorized access to any computer or network systems. This includes unauthorized probes, scans, or attacks of any kind.
7. Do not attempt to read, copy, modify, or delete any data or information unless you have permission to access it. This applies even if the data or information is not protected.
8. If you have reason to suspect an unauthorized access on any system, contact the System Manager or Police Services, x5472, (available 24 hours daily).
9. If you have any questions about these rules, or any computer security matter:
 - 1• Consult the Computer Security Web Pages (<http://www.lbl.gov/cyber>)
 - 2• Contact your supervisor
 - 3• Contact the System Managers of the system involved
 - 4• Contact the LBNL Computer Protection Program (cppm@lbl.gov)

I have read and understand the foregoing computer security rules. I understand that failure to comply with these rules can result in disciplinary action including possible termination of employment at LBNL.

Signature: _____ Date: _____

Print name: _____