Proper Use of LLNL Computers

Statement of Policy
The following rules apply to all users of LLNL classified and unclassified computers; individual organizations may apply additional rules to the use of their resources, provided these additional rules are not in conflict with this policy. Questions concerning organization-specific rules should be addressed to your supervisor, manager, Information System Security Officer (ISSO), or Organizational Information System Security Officer (OISSO).

Please see the References section for additional information pertaining to the following rules.

Authorized Use: Only authorized individuals may use LLNL computers. Users should not exceed authorized access.

Unclassified Environment
- LLNL employees who are U.S. citizens are granted access to use LLNL computers
- Non-employees who are U.S. citizens must receive authorization before using any LLNL unclassified computers. This authorization must come from either the host program or the contract between the Lab and the person's employer.
- Persons who are not U.S. citizens, regardless of employment status, must have approved F-2311 and F-2312 forms in place before using any LLNL unclassified computers. In addition, non-U.S. citizens may only access those computers listed in the approved F-2311 form.

Classified Environment
Prior to being approved for access to a classified resource and annually thereafter, users must:
- complete training on classified computer use (CSP training class: CS0115-W) in order to achieve, acknowledge and maintain awareness of their responsibilities for protecting classified information systems and classified information; and
- obtain approval for access from the organization responsible for the resource (a record of this approval is retained by the resource’s system administrator and/or ISSO).

Personal Use: Personal use of computers is either limited or prohibited at LLNL, according to the following:

Unclassified Environment
Only LLNL employees may make personal use of LLNL unclassified computing resources, if in accordance with the LLNL Human Resources Personnel Policies and Procedure Manual, Section D: Employee Conduct, III: Incidental Personnel Use of Unclassified Information Technology Resource Policy. For example, certain computing
activities are strictly forbidden. You cannot create, download, view, store, copy, transmit, or retransmit:

- unauthorized mass mailings, (e.g., chain letters)
- sexually explicit or sexually oriented materials or images
- materials that support gambling, illegal weapons, terrorist operations, or criminal activities.

**Classified Environment**
Personal use of LLNL classified computing resources is prohibited.

**Authorized Actions:** Users of LLNL computer systems may use those resources only in a manner approved by the institution and their respective programs. Examples of unauthorized actions include, but are not limited to: reading, altering, or destroying information to which the user is not authorized access; and actions that deny legitimate access by authorized personnel to a system or service.

**Privacy:** Users have limited privacy when using LLNL computers, in accordance with the DOE directive (CIAC Bulletin J-043). This directive is displayed either in hardcopy or as a login banner on all LLNL computers.

**Software Licenses:** All software used on LLNL computers must be appropriately acquired and used according to the applicable licensing agreements.

**Classified Environment**
Prior to its installation and use on classified systems, software must be approved (generically or specifically) by the appropriate ISSO. Reference: LLNL Personnel Policies and Procedures Manual Section D VIII.5.

**Passwords:** Computer passwords must comply with the rules in NNSA NAP 14.2-B, Chapter C: Password Generation, Protection, and Use. Users must ensure that passwords (including any authentication mechanisms) issued for the control of their access to information and information systems are not shared and are protected at the same level of protection applied to the information to which it permits access.

**Classified Environment**
Classified computer passwords must also comply with the rules in LLNL Policy P-4310 and DOE M 471.2-2.

**Modems:** Use of modems is either limited or prohibited at LLNL, according to the following:

**Unclassified Environment**
The Open Terminal Server (OTS) modem pool is the only approved method of accessing unclassified LLNL computers and networks via modems. All unclassified computer systems with modems, other than Facsimile (FAX) machines, must be configured with auto-answer turned off.

**Classified Environment**
Modems are prohibited on classified systems.

**Installing Software on computers:** Extreme caution must be used to install non-LLNL supplied software on unclassified computer systems. External software, such as freeware or public domain software, is often bundled with adware/spyware which is a security risk for LLNL system. This is true for some screensavers from Web Shots or
other locations which is not allowed. Check with your ISSO, OISSO or CSP prior to installing any unclassified software.

Installing non-LLNL supplied software on classified computer systems is strictly controlled. Classified ISSOs must keep an auditable record of any public domain software. This software must be approved by the ISSO.

**Changing Security Settings:** Computer (desktop, laptop, server, etc.) security settings are pre-defined and are not to be modified. Operating system (OS) configuration settings and images have been established and are certified annually for compliance. Only LLNL systems administrators are allowed to modify any pre-defined settings. Refer any questions to your OISSO, ISSO or CSP.

**Laptop Travel Restrictions:** LLNL has restriction on laptops used outside of the facility. Requirements are established for taking LLNL portable computers on travel to Foreign Countries including countries on the DOE Sensitive Countries list. Refer to CSP policy 2360, “Taking LLNL Portable Computers on Foreign Travel Policy”, for this requirement. Furthermore, restrictions are also established for the responsibilities of LLNL employees with regard to the protection of Personally Identifiable Information (PII) on laptops and removable media that leave LLNL facilities. Refer to the Security Organization policy SSO-POL-012, “Protection of LLNL Personally Identifiable Information Policy”, for this requirement.

**Virus Protection:** All unclassified and classified systems must, where technically feasible, use anti-virus/malicious code software. Refer to CSP policy 2022, “Baseline Unclassified System Management and Configuration” for this requirement on unclassified systems and CSP policy 4351, “Protecting Classified Computers Against Viruses and Malicious Code” for this requirement on classified systems.

**Social Engineering:** Social engineering is a term describing a non-technical attack that relies heavily on human interactions and involves “tricking” computer users into breaking normal security procedures. Social engineers use numerous techniques using phone calls or email to obtain information. Use extreme caution releasing information of any form. Contact your ISSO, OISSO or CSP for further information.

**Spam and Spyware:** LLNL detects and mitigates most spam and spy-ware with the implementation of software products such as the Blue Coat Web Proxy and BrightMail SPAM filtering tools. However, occasionally a new computer worm or virus comes through the Laboratory’s unclassified cyber security defenses undetected, which could result in a compromise of computers. This is a reminder that the threat of comprehensive, malevolent attacks is continuous and high. The following are recommendations to help protect LLNL network and computers from malicious activities:

- Don’t open unknown e-mail attachments or click on suspicious links.
- Ensure that your computer has the most recent operating system security patches.
- Ensure your antivirus application is installed, functioning, and updated with the latest software.
• Ensure that your computer scans all files for viruses.

**Encryption:** Unclassified Controlled Information (UCI), formerly known as Sensitive Unclassified Information (SUI), is unclassified information requiring control with respect to transmission and encryption. UCI, as defined and applied at LLNL, embraces eight categories of information, listed below.

- Unclassified Controlled Nuclear Information (UCNI)
- DOE-defined Official Use Only (OUO)
- Personally Identifiable Information (PII)
- Naval Nuclear Propulsion Information (NNPI)
- Export Control Information (ECI)
- Applied Technology (AT)
- Reactor Safeguards Information (RSI)
- Confidential Foreign Government Information--Modified Handling Required (C/FGI-MOD)

Additional information about any of the above UCI category and the encryption requirement can be found at the UCI website (https://uci-r.llnl.gov/).

**Computer Security Incidents:** It is the responsibility of all Laboratory employees, contractors, sub-contractors, guests and visitors to report any suspected or actual computer security incident as soon as possible to the ISSO responsible for the resource. The ISSO will report it to the LLNL Computer Security Program (CSP). If the ISSO is not available, then the suspected or actual computer security incident should be reported directly to CSP. CSP will coordinate the investigation with the appropriate internal and external parties (see LLNL Policy P-2316).

**Effective Date**
This policy is effective on the date of its approval.

**Exceptions**
Exceptions to this policy may be sought from the CIO by application to the LLNL CSP Office.

**Consequences of Non-Compliance**
Failure to comply with this policy, without an approved exception, may result in administrative or corrective actions up to and including dismissal.

**Attachments**

**Glossary**
Please see [Computer Security Policy Glossary](#).
Background
The users of LLNL computer systems play a very important role in the overall computer security program at LLNL. To execute this role satisfactorily, users are expected to abide by certain standards of conduct when using those systems. In addition, they must be aware of certain basic expectations and policies governing their use of such systems. This document codifies those standards and expectations.

References
CS0115-W: Training for Users of Classified Information Systems
P-2023: Incidental Personal Use of Unclassified Information Technology Resources
P-2025: Protecting Unclassified Systems against Viruses and Malicious Code
F-2311: Computer Security Plan for Foreign National Visitors & Employees
F-2312: Computer Security Responsibilities for Hosts of Foreign National Visitors or Assignees
P-2316: Reporting Computer Security Incidents to LLNL Computer Security Operations (CSO)
IM-4310: Classified Computer Password Management Requirements
P-4351: Policy for Protecting Classified Computers from Viruses and Malicious Code at LLNL
SSO-POL-012: Protection of LLNL Personally Identifiable Information Policy
CL0010: Export Control at LLNL
J-043: CIAC Bulletin
NNSA NAP-14.1-B: NNSA Cyber Security Program
NNSA NAP-14.2-B: Baseline Cyber Security Requirements

Policy History
20 Sep 2001 v3.0 Merged P-2329 with previous version of this policy
08 Jan 2003 v3.1 Revised Authorized Use section for classified users; cancelled P-4336; added link to CS0115-W
07 Dec 2007 v3.2 Update policy due to Network section being moved to P-2401
12 June 2012 v3.3 Updated misspelled words