

## Managing Computer Hardware

Keep track of all your computer equipment “cradle-to-grave.” Periodically check your Property Accountability Statement, verifying the location of all equipment. NEVER transfer or dispose of equipment without contacting your OCSR and Property Representative for help.

## Classified Processing

If you process classified information on a computer, remember these important rules:

- Cyber System Security Officers (CSSOs) manage classified computing equipment. Computers used to process classified information MUST have a current approved security plan, test plan, and accreditation **BEFORE** use.
- Classified computer users must complete the Classified Computer Security Briefing (online course #17846).
- Classified systems require more stringent minimum protections; these protections are outlined in the security plan.
- The data owner is responsible for ensuring that information is not accessible to unauthorized individuals. In order to access classified information, proper clearance level and need-to-know authorization is required.
- Those handling ACREM (Accountable Classified Removable Electronic Media) must undergo ACREM training, demonstrate an understanding of the rules, be authorized by the Security Responsible Line Manager (SRLM), and follow the prescribed rules for storage.
- Do **NOT** install software or introduce non-LANL media to a classified system without the CSSO’s authorization.

Your OCSR or CSSO must be consulted before ANY processing of classified information.

## Protecting Information

Properly identify and familiarize yourself with the level of information you process, and protect your computer and information at the highest possible level. Only those with a need-to-know should have access to the data on your computer. Sensitive information files identified as UCNI or OOU require special protections.

URL: <http://int.lanl.gov/security/protectinfo/>

## Personally Identifiable Information

Personally Identifiable Information (PII) about an individual can be used to distinguish or trace an individual’s identity. Examples include social security numbers, date, place of birth, mother’s maiden name, financial account numbers, PINs, and biometric information.

If you process PII, there are requirements for managing the data. Any data sent or carried offsite (e.g., by e-mail, a laptop, or a thumb drive, etc.) must be encrypted. Immediately report any potential loss of PII to the Security Inquiry Team at 665-3505.

<http://int.lanl.gov/security/cyber/access/pii.shtml>

## Information Security Contacts

Phone: 665-1795 Fax: 665-1799

E-mail: [cybersecurity@lanl.gov](mailto:cybersecurity@lanl.gov)

URL: <http://int.lanl.gov/security/cyber/>

## Wireless Connections and Networks

E-mail: [wirelesssecurity@lanl.gov](mailto:wirelesssecurity@lanl.gov)

URL: <http://int.lanl.gov/security/cyber/computer/wireless.shtml>



Los Alamos National Laboratory, P.O. Box 1663, Los Alamos, NM USA 87545  
Los Alamos National Laboratory, an affirmative action/equal opportunity employer, is operated by the Los Alamos National Security, LLC, for the United States Department of Energy under contract DE-AC52-06NA25396.

LALP-08-061

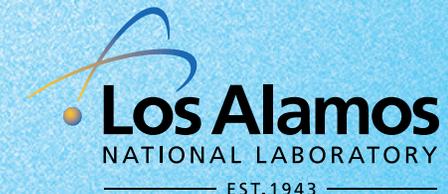
October 2008



# Quick Reference Card for Users

October 2008

<http://int.lanl.gov/security/cyber/>



## Are You a Computer User?

You are a computer user if you use LANL-owned computer resources, connect to a LANL network, or use the LANL network to get e-mail. You are NOT a computer user if you ONLY access Laboratory computer resources to complete required training.

## Computer Resources

Laboratory computer resources are to be used for official purposes ONLY and are subject to monitoring and inspection. Inappropriate use may result in disciplinary action. Examples of waste, fraud, and abuse include, but are not limited to the following:

- Accessing pornography or gambling sites,
- Downloading music,
- Running a home business, or
- Excessive Web “surfing.”

## Who is Your Group OCSR?

Get to know your Organizational Computer Security Representative (OCSR) (commonly called “Oscar”). Your OCSR is a good resource for information security assistance.

<http://int.lanl.gov/security/cyber/docs/OCSR/ISSO.xls>

## Required Training

All computer users must complete the Initial Information Security Briefing (online course #9369).

<http://www.lanl.gov/training/s-courses/9369/splash-in.asp>

Users must complete the Annual Information Security Refresher (online course #47075) on a yearly basis.

<http://www.lanl.gov/training/s-courses/47075/splash-in.asp>

## User Registration

All Laboratory computer users must register as soon as possible after being granted computer access.

A cryptocard with administrative-level authorities is required for computer users to register online.

If you don't have these authorities, contact your OCSR to get registered. During the registration process, print or save an electronic copy of the following:

- Computer Security Responsibility Acknowledgment and
- Computer Security Profile.

Once a year, review your registration, especially if your job or assignment has changed.

<http://int.lanl.gov/security/cyber/registration.shtml>

## Minimum Information Security Protections

- Follow Laboratory password guidelines; see P218, Cyber Security Access Controls.
- Enable screensaver protections when away from your computer.
- Enable virus protection software with up-to-date definitions installed; scan for viruses regularly.
- Remember to back up your files regularly.
- Verify licensing for all your software.
- Report questionable events and potential incidents to the Security Inquiry Team (SIT) and to your OCSR.
- Manage computer equipment in accordance with established Laboratory guidelines.
- Disable *all* wireless networking capabilities (802.11x and Bluetooth).
- Never open e-mail attachments or click on URLs from unfamiliar sources. Some attachments are infected with worms and viruses.

- Do not respond to “phishing” attempts (e-mail requests for personal and/or sensitive information). Financial service providers (e.g., your bank or credit card company) will never ask for sensitive information through e-mail.

## Information Security Incidents

If you discover a potential information security incident (such as attempted unauthorized access to your system, sharing of passwords, contamination of an unclassified system with classified information, etc.), immediately report it to the Security Inquiry Team at 665-3505, your OCSR, and line manager.

**Your OCSR will work with information security professionals to address the problem.**

## Portable Electronic Devices (PEDs)

PEDs can store and/or transmit data.

Restrictions are placed on the use of PEDs, depending on the following:

- **Owner** of the device (government or non-government) and
- **Where** the device will be used (open or limited area, classified computing areas).

PEDs consist of the following:

- **Controlled Article (CA)**—A device that operates independently from a computer (laptops, iPods, portable data assistants, etc.) and
- **Portable Electronic Storage Device (PESD)**—A device that operates when connected to a computer (such as a thumb drive, CD/DVD write drives, flash memory cards, external hard drives, etc.).

Form 1897 is used for requesting approval for the use of restricted devices. See P217, Portable Electronic Devices.