



Policy 2028 v1.2
December 17, 2007

Protecting LLNL Employee Remote Computer Systems

Statement of Policy

LLNL employees will not remotely access LLNL networks unless their remote access computer meets or exceeds standards set within the Unclassified Master Plan "LLNL MSP-GSS-1". Each year, employees will affirm that they comply with these minimum configuration standards. This restriction applies to all computers used for such access.

Purpose

Protect remote access computers from Internet threats and increase the LLNL network security.

Background

Unprotected home and travel computers (particularly those with broadband, "always-on" links) are easy targets for viruses, worms, and hackers. The security of remote computers is increasingly important to the overall security of LLNL's computer networks.

Recommendations

Appendix B provides recommendations to remote computer users processing LLNL information. To protect "always-on" remote computers from Internet hackers, use hardware or software firewalls, including Network Address Translation (NAT) routers. Such routers convert a non-routable private address to a public IP address allowing user access to the Internet and help to prevent unauthorized access from the Internet. Hackers will thus only "see" the router and not the systems behind the router.

Implementation and Funding Plan

The Cyber Security Program (CSP) will create and maintain minimum security baseline standards for remote access computing. Remote access users will be responsible for complying with these requirements. Directorates may develop additional procedures to support remote access users in meeting these requirements. CSP will modify the remote access account procedures to require users to annually reaffirm their responsibilities for the security of their remote systems and the LLNL data on these remote systems. The account management for access is provided by the CSP Remote Access Account Management System (AAMS). The Organizational Information System Security Officer (OISSO) or their designees are responsible to create the account after CSP Form 2410 has been approved. Forms are filed by each OISSO and accounts then managed by the AAMS software. Users are notified of their responsibilities initially via the Form 2410 and then annually by AAMS generated email.

Consequences of Non-Compliance

If a remote system is discovered to be out of compliance with this policy, the user's remote access to the Yellow Network will be suspended and both the employee's Associate Director and the Laboratory's Chief Information Officer (CIO) will be notified.

There will be no restoration of such remote access until the employee provides evidence that the involved computer system is in compliance with this policy.

Failure to comply with this policy, without an approved exception, may also result in other administrative actions up to and including dismissal.

Effective Date

This policy is effective on the date of approval.

Exceptions

The Cyber Security Site Manager may grant exceptions to this policy.

Additional Information**Glossary**

Please see [Cyber Security Glossary](#).

References

Additional computer security guidance is available at <https://www-csp.llnl.gov/csphome.html>

National Institute of Standards and Technology (NIST) special publication 800-46 (<http://csrc.nist.gov/publications/nistpubs/800-46/sp800-46.pdf>).

“Remote Internet Security for Home and Portable Systems”, written by the Burton Group under contract to the University of California.

Cancellations

None

Policy History

19 Mar 2004	v1.0	CPAC and CIO approved original
04 May 2007	v1.1	Revised and Updated by CSSM
17 Dec 2007	v1.2	Added wording regarding the AAMS and annual affirmation.

Appendix A

Standards for Remote Access Computers

Anti-Virus Software

If you are using a Windows PC or Mac, make sure your computer is protected by anti-virus software that provides real-time protection like the Laboratory's site-licensed Symantec Anti-virus (SAV) version 10.X found at <https://smsg/norton/index.html>. The Laboratory's site licensed software can be installed on LLNL-owned systems only. The Laboratory's site-licensed software cannot be used on personally owned systems. A legal copy of anti-virus software must be acquired for non-LLNL owned systems. Be sure your anti-virus software is configured to update its virus definitions daily and conduct periodic scans of all associated disks.

Hardware/Software Firewall or Router that Performs the NAT function

Hardware/Software firewalls or routers should perform the Network Address Translation (NAT) function and be:

- Configured to hide home computer IP addresses.
- Configured to accept only specifically identified inbound connection requests (sometimes known as paranoid mode or "default deny").

Make sure your computer is protected by a firewall. If you are not protected by a hardware firewall, ensure the Operating System (OS) firewalls in Windows and Macs are turned on. For non-LLNL owned systems, Zone Labs offers a free software firewall that can be downloaded from

http://www.zonelabs.com/store/content/catalog/products/sku_list_zainfo

Securing Wireless Networks.

When used, the following requirements apply.

- Can only use Virtual Private Network (VPN) access.
- At a minimum, enable 128 bit Wired Equivalent Privacy (WEP) encryption.
- Change SSID from default value.
- Disable broadcasts of Service Set Identifier (SSID) in the wireless base station beacon message.

Appendix B

Recommendations for Remote Access Computers

Patch Systems

Systems should have all current security patches.

- If you have system administrator/root privileges on the computer, it is your responsibility to make sure the computer security patches are kept up to date.
- If you don't have system administrator/root privileges, you must work with your LLNL system administrator to establish a procedure for patching the system.

Keeping the operating system and applications patched is critical to the security of the system. Some operating systems check automatically for updates. If your system is not capable of checking automatically for security alerts, you will have to periodically check the vendor's web site.

Securing Wireless Networks – additional recommendations

- Place wireless base station away from outside walls in order to minimize transmission of data outside of building.
- Disable SNMP or change the SNMP community strings to a hard-to-guess password.

Encryption Software

Always use VPN client software.

Backup Data

Backup your data frequently.

Other Precautions

- Secure or disable file and printer sharing.
- Use a password protected screensaver to lock your computer during periods of inactivity.
- Turn your system off when it is not being used.