BROOKHAVEN NATIONAL LABORATORY

BNL Computer Use Agreement

Introduction

This agreement applies to all users of Brookhaven National Laboratory's computer resources, which include Laboratory owned computers, computer systems, networks, storage, printers and portable/mobile devices, as well as all methods of access, whether local or remote. Computer resources are provided to support the Laboratory's official business.

Privacy

The Laboratory monitors its computer resources to detect improper use. Investigation of detected improper use may result in confiscation of the offending device for confirmation and evidence gathering by appropriate authorities.

Use of the Laboratory's computer resources implies consent to review and disclose information and usage upon violation of this agreement or when mandated by law. Violations will result in consequences including, but not limited to, loss of access to computer resources, administrative disciplinary action, and civil and criminal penalties.

Responsibilities

- Be aware of, knowledgeable about, and comply with the requirements of the BNL Cyber Security Program as described in SBMS.
- Follow BNL policy regarding the use and protection of accounts and passwords.
- Protect sensitive information and Personally Identifiable Information (PII) in accordance with the requirements set forth in the Operations Security (OPSEC) and PII SBMS Subject Areas.
- Observe licensing and other computer-related contract provisions - particularly those that could expose the Laboratory to legal costs or damages if not followed.
- Ensure that computers under your control have virus-protection software installed and kept up to date.
- Keep computing systems properly configured and patched to remain compliant with current cyber security requirements. This function may be delegated to local system administrators or central IT staff.
- Participate in cyber security training and awareness.
- Report suspicious activity or known security violations to the Cyber Security Incident Response Team, security@bnl.gov or the Cyber Security Hotline at extension 8484.

Limited Personal Use

There is no inherent right for the personal use of the Laboratory's computer resources however limited use for personal purposes is allowed under the following criteria:

- Involves minimal additional expenses to the Laboratory.
- Does not interfere with the mission and operations of the Laboratory, interfere with job performance or delay or compromise the Laboratory's projects.
- Does not compromise information security.
- Does not involve illegal activities.
- Does not involve operating a private business or supporting any political enterprise.
- Does not involve activities that could potentially embarrass the Laboratory or the DOE.
- Does not give the impression of acting in an official capacity when using computing resources for personal purposes.

Personal use may be restricted if the above criteria are violated and personal use of classified computer resources is not permitted.

Appropriate Use

The following examples of personal use of Laboratory computer resources constitute acceptable activities that meet the criteria specified above.

- Ongoing education, self-training, and professional development.
- Personal correspondence and work on your own resume or those of family members.
- Work for charities and non-political local community groups.
- Good-taste Internet access.
- Limited use of instant messaging or internet-based phone programs.
- Research activities, such as reading newspapers and magazine articles, checking airline prices and schedules and purchasing tickets, browsing sales catalogs, comparing prices of automobiles, obtaining road maps, and checking accounts in credit unions and retirement plans.

- Occasional personal banking such as managing checking and savings accounts online or reviewing your retirement portfolio.

If you are unsure whether certain personal use of Lab computing is appropriate, contact the Cyber Security Office for clarification via email to security@bnl.gov or through the Cyber Security Hotline at x8484.

Inappropriate Use

The following are examples of inappropriate use of Laboratory computer resources and are prohibited.

- Accessing content that promotes hate language, harassments, or threats.
- Accessing content that ridicules others on the basis of race, creed, religion, sex, disability, nationality, or sexual orientation.
- Creating, downloading, viewing, storing, copying, or transmitting sexually oriented or sexually explicit material (e.g., pornography, child pornography)
- Gambling.
- Working for commercial purposes or supporting for-profit organizations that are outside the scope of your BNL appointment.
- Recommending products or services as being endorsed by BNL.
- Participating in any partisan political activity.
- Misleading someone into believing you are acting in an official capacity.
- Hosting services (such as web sites) that are not of general interest to the Laboratory.
- Using prohibited peer-to-peer (P2P) file sharing services, such as those listed at http://www.bnl.gov/cybersecurity/p2p.asp.
- Circumventing the perimeter firewall in a way that allows an internal machine to be accessed from an external, insecure network without first obtaining approval via the Cyber Security Management Information System. Example is forwarding an internal port to an external network.
- Creating and/or forwarding of chain letters and unrequested bulk email (SPAM).
- Using software, such as password-cracking tools and vulnerability scanners, without the consent of the Information Systems Security Manager (ISSM).
- Intentional use of software or techniques meant to disguise or circumvent the detection of computing activities on the BNL network.

This list should not be considered all-inclusive; please check with the Cyber Security Office about your proposed usage. Please reference DOE Order 203.1 “Limited Personal Use of Government Office Equipment Including Information Technology” for additional information and guidance.

References

- DOE Order 203.1.4.a, "Limited Personal Use of Government Office Equipment Including Information Technology"
- 10 CFR Part 727, "Computer Security; Access to Information on Department of Energy Computers and Computer Systems"
- SBMS Unclassified Cyber Security Subject Area
- SBMS Interim PII Subject Area
- Operations Security (OPSEC) SBMS Subject Area

Signature

All users are required to have a signed copy of this document on file with Human Resources prior to using BNL computer resources.

By signing this form you are acknowledging that you have read, understand, and agree to comply with the above principles governing the use of Brookhaven National Laboratory computer resources. Updates made to this agreement will also apply with notification of changes made through the BNL SBMS change notification process. The official copy of this agreement is located in the BNL SBMS system.

Signature: _____ Date:_____

Print Name:_____ Life/Guest #:_____