



Memo

Date: November 9, 2007

To: All Employees

From: Sam Aronson 

Subject: Appropriate Computer and Networking Use

Since we continue to encounter instances of inappropriate computer use by employees, users, and guests, I want to remind everyone about the Laboratory's policy on the use of computers and networking resources. This policy applies to all forms of on-site computer and networking use, regardless of machine ownership. It includes use of Government-issued desktop, laptop, and hand-held computers, and also applies to all employee/user/guest-owned computers using BNL networking resources, such as internet access, anywhere on site.

BNL computer and network resources are U.S. Government property and are provided by the Laboratory to our employees, visitors, and guests primarily for business purposes. BNL policy prescribes that a "reasonable level" of personal use of these resources is acceptable, provided that such use is appropriate. Employees must also ensure that such use does not impact or interfere with their job performance. Examples of appropriate personal use include:

- Good-taste internet access, 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
- Ongoing education, self-training, and professional development
- Personal correspondence and work on your own resume or those of family members
- Limited use of instant messaging or internet-based phone programs
- Work for charities and non-political local community groups
- Work on personal finances (for example, preparing income taxes).

Employees, visitors, and guests must also be aware of and avoid situations of inappropriate or illegal uses of all Government equipment. Examples of inappropriate use of computing and networking resources that are strictly prohibited include:

- Creating, downloading, viewing, storing, copying, or transmitting sexually oriented material (e.g., pornography, child pornography)
- Supporting or accessing sites that promote hate language, harassments, or threats

- Supporting or accessing sites that ridicule others on the basis of race, creed, religion, sex, disability, nationality, or sexual orientation
- Gambling
- Working for commercial purposes or supporting for-profit organizations or other outside employment or businesses
- Endorsing any product or service
- Participating in any partisan political activity
- Misleading someone into believing you are acting in an official capacity
- Hosting services (such as creating or storing web sites) for purposes not related to Brookhaven's work
- Using peer-to-peer (P2P) file-sharing services, such as BitTorrent, Gnutella, and KaZaA.
- Using any tool or method, such as external proxies, to bypass cyber security controls.
- Using any software that allows your computer to be shared outside the Brookhaven firewall without first obtaining approval via the Cyber Security Management Information System
- Using Internet auction sites, such as eBay, for personal use
- Creating and/or forwarding chain letters and mass mailings
- Violating license and other computer-related contract provisions, particularly those that expose the Laboratory to legal costs or damages, like downloading "cracked" software from so-called "warez" sites
- Using software, such as password-cracking tools, vulnerability scanners, and network sniffers, without the express written consent of the Computer Protection Program Manager.

Employees, users, and guests must also be aware that there should be no expectation of privacy on Government-owned computers. E-mails and computer files may be reviewed at the discretion of the Laboratory. In addition, the Laboratory employs advanced scanning tools that detect inappropriate internet use. If you are accessing the internet anywhere on site and disobey these guidelines, you can expect to be caught.

Employees found violating these guidelines will be (and have been) subject to disciplinary actions ranging from suspension without pay to termination. The Laboratory is also required to report certain specific inappropriate activities, such as those involving child pornography, to external law enforcement agencies for further investigation. If you believe you are suffering from an internet addiction of any kind, please seek help from the Lab's Employee Assistance Program, Ext. 4567.

Details of the policy can be found at https://sbms.bnl.gov/sbmsearch/subjarea/61/61_Pro2.cfm and http://www.bnl.gov/cybersecurity/user_agreement.asp. The lists of appropriate and inappropriate uses above are not all-inclusive; if you have any questions about a particular use, please contact the Cyber Security Office at Ext. 8484.