Unacceptable Use of NIST Information Technology Resources

Unacceptable Use of NIST Information Technology Resources includes, but is not limited to:

(a) Commercial or business use for the profit of an individual, or company, or other activity that is not approved by a NIST manager as essential to the NIST mission;
(b) Any activity that has not been authorized, or in a manner that knowingly violates the policies of the owner of the network or system;
(c) Any activity that interferes with the normal operation of a NIST system or network, including denial of service attacks or use of privileged commands on a NIST system.

Enforcement

The enforcement of the unacceptable use policy is based on the specific circumstances of each case. NIST management may take any action it deems necessary to protect the NIST systems and networks. This may include legal action, such as criminal prosecution or civil penalties. NIST management may also take administrative action, such as suspending or terminating access to NIST systems or networks.

Policy on Access and Use

NIST expects users to conduct themselves professionally and refrain from using NIST resources for activities that are likely to be offensive to coworkers or the public. Some examples include:

(a) use of NIST information technology resources to engage in illegal or unethical activities;
(b) use of NIST information technology resources to promote or support activities that are likely to be offensive to coworkers or the public;
(c) use of NIST information technology resources to access or propagate content that is likely to be offensive to coworkers or the public.

Privacy of Information

NIST uses its best efforts to ensure the privacy of information in its possession. NIST employees are required to follow NIST guidelines for downloading and using information technology resources. NIST also takes reasonable steps to protect the privacy of its customers and the public.
This section describes uses of NIST information technology systems that are considered acceptable by NIST management. The general criteria used in deciding acceptable use are whether the use of NIST information technology resources that are not explicitly mentioned in this policy should be directed to NIST management.

NIST information technology resources may be used in the conduct of NIST research, in the administration and management of NIST programs, and in the dissemination of the results of NIST work. Examples of such use of NIST information technology include, but are not limited to:

- Computation, modeling and simulation, and support of experiments needed to accomplish NIST research, including research on information technology systems;
- Analysis and storage of data, including experimental data, output from models, and administrative data;
- Visualization of the output from models and experiments;
- Preparation of reports, papers, memos, correspondence, databases, graphics, displays, presentations, and any other products of NIST work;
- Management of NIST operations and staff.

NIST information resources may be used to communicate and exchange information with others located at NIST, and elsewhere, to share information related to the NIST mission. This includes researchers at other institutions, customers in industry, and government agencies, other government agencies, and the public.

Examples of acceptable communications include:

- Disseminating appropriate information related to NIST mission topics electronically to our customers in industry, government, universities, and the public around the world;
- Communicating by electronic mail or other means with research colleagues, customers, other government agencies, and vendors for purposes of NIST business;
- Accessing public information available on the Internet, or elsewhere, related to NIST research and the mission of NIST;
- Obtaining software patches, and updates from vendors, public domain software repositories, and other sources, provided that the software is installed in accordance with U.S. copyright regulations, the license for that software, and NIST security policies;
- Participation in forums, newsgroups, and other information exchanges for the purpose of improving the professional knowledge or skills of NIST staff.

Software from the Internet and other public sources, and installing unnecessary software from any source, increases security risks to NIST networks and computers by...

To ensure accountability of actions and resources, each person who has access to a NIST information technology system must have an individual account. Sharing of accounts and passwords must follow the guidelines established by the NIST IT Security Office when downloading software from the Internet:

- Only install software that will be used for work-related functions.
- Only install or run software that was written by well-known, established sources. At a minimum, you should be able to identify the author or company that wrote the software and validate that you can locate and communicate with the author or company to discuss problems that might arise.
- Make sure anti-virus software is installed, set to auto-protect, and maintained with current anti-virus definitions before installing any software on NIST computers.
- Scan downloaded files for viruses before installing and running them. Generally, shrink-wrapped commercial software should be virus-free (although some manufacturers have distributed infected software).
- NIST software may be installed on non-NIST computers for work-related purposes (e.g., to work from home). NIST software... This requirement does not apply to NIST software where the software usage license allows for free public distribution.

NIST communications facilities may be used to provide access to NIST information technology systems and those of other organizations for authorized purposes. Examples of authorized access to systems include:

- Access to NIST systems and networks from off-site locations for users with specific needs for such types of access, such as access when on travel or from home;
- Access to academic, government, and industrial computer systems for accomplishing joint projects, where that access is authorized by the owner;
- Access to academic computing facilities for taking courses.

To ensure accountability of actions and resources, each person who has access to a NIST information technology system must have an individual account. Sharing of accounts and passwords...

General access to public NIST information technology resources, such as Web, Bulletin Boards, public anonymous ftp, Mosaic, gopher, or other services used by NIST to...

NIST provides access to information technology resources, including computers, networks, and peripheral devices, to support the NIST mission. The following guidelines apply to all users who use NIST information technology resources:...
I have read, and understand the document titled, "NIST Policy on Information Technology Resources Access and Use," dated October 2003, and agree to abide by this and all NIST IT security-related policies.

_________________________________  Date: _______________
Signature:_________________________  Date: _______________________

Please sign, date, and return this page to: NIST ITAC, Mail Code 1820

_________________________________  Provided orientation (initial/date): ______________________
Name (First name / Last name): ____________________________

_________________________________  Entered into certification database: _________________________
Division Name and Number: _______________________________

_________________________________  Organization Unit: ______________________________________

FOR OFFICIAL USE ONLY

NIST UID: _________________________________________

NIST Policy on Information Technology Resources Access and Use