www.nist.gov/director/nist-policy-%25C2%25A0information-technology-resources-access-and-use

National Institute of Standards and Technology
U.S. Department of Commerce

Office of the Director (https://www.nist.gov/director)

NIST Policy on Information Technology Resources Access and Use

Originally Posted: October 8, 1998
Updated: February 21, 2003
Updated: October 2003
CIO Approved: October 10, 2003

Policy:

All information technology users must sign a document (https://www.nist.gov/director/oism/itsd/upload/memo_accessnuse_sign.pdf) stating that they acknowledge having read, and agree to abide by, this policy.

Introduction

NIST provides access to information technology resources, including computers, networks, and peripheral devices, to support the NIST mission. The following guidelines apply to all who use and access NIST information technology resources.

Acceptable Use of NIST Information Technology Resources

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 application is of benefit to NIST, whether it complies with government laws and regulations, and whether it does not adversely affect others. NIST allows the personal use of the Internet as long as it does not interfere with official business, increase cost to NIST or embarrass NIST. Questions about 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 elsewhere, vendors and companies with products of interest to NIST, 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 such software is obtained, checked and tested, and installed in accordance with U.S. copyright regulations, the license for that software, and NIST security policies;
- Participation in forums, news groups, and other information exchanges for the purpose of furthering the NIST mission or 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 potentially including things such as harmful viruses, back doors, and mechanisms specifically designed to defeat firewall protection. Users 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 original source of 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 free from viruses (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 must be removed from non-NIST computers when the information technology user is no longer associated with NIST or when the information technology user no longer needs the software for work-related purposes. This requirement does not apply to NIST software where the software usage license allows for free public distribution.

Acceptable Access to Information Technology Resources

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 or authorization methods is prohibited, except in special cases such as e-mail accounts for the operation of special services supported by a team of people. Access to NIST information technology resources requires formal written authorization by a user's manager. The authorization should specify the duration of the access to the NIST resource, acceptable use of the NIST resource, and a rationale for granting access to NIST information technology resources. A copy of the authorization and a copy of this policy should be given to the user.

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 disseminate information to the public requires no special authorization. However, misuse of these services or attempts to exceed authorized access is subject to the same penalties as other unacceptable uses described below.

Unacceptable Use of NIST Information Technology Resources

The use of NIST systems and networks in a manner which is unacceptable may subject the person(s) involved to loss of all privileges to use NIST systems, may result in other disciplinary sanctions up to and including dismissal, or may result in criminal prosecution. Unacceptable uses of NIST systems and networks include, but are not limited to:

- Commercial or business use for the profit of an individual, or company, or other use of NIST systems not approved by a NIST manager as essential to the NIST mission;
- Any use of NIST information technology resources in order to obtain access to any network or system at NIST, or elsewhere, for which the person has not been authorized, or in a manner that knowingly violates the policies of the owner of the network or system;
- Any activity that interferes with the legitimate activities of anyone using any NIST systems or networks, or any other network or system which may be accessed from NIST;
- Unauthorized use of a system for which the user has authorized access, including use of privileged commands on a system by a user not authorized to use such commands and unauthorized access to information owned by someone else. For example, no user may access the root account on a Unix system or attempt to become root on the system unless he or she is authorized to do so;
- Deliberate unauthorized destruction of NIST data or other resources;
- Any use of NIST information technology resources to engage in illegal or unethical activities;
- NIST expects users to conduct themselves professionally and to refrain from using NIST resources for activities that are offensive to coworkers or the public. Some examples include the use of NIST IT resources that contain or promote (a) matters directed toward the success or failure of a political party, candidate for partisan political office, or partisan political group, (b) engaging in any action supportive of lobbying the Congress, (c) use of Internet sites that result in an unauthorized charge to the Government, (d) participating in prohibited activities such as discriminatory conduct, gambling, and disseminating chain letters, (e) intentional and unauthorized viewing of sexually explicit or pornographic material, (f) sending personal e-mail that might be construed by the recipient to be an official communication, (g) any activity that would bring discredit on NIST or the Department of Commerce, (h) statements viewed as harassing others based on race, age, creed, religion, national origin, color, sex, handicap, or sexual orientation, (i) any violation of statute or regulation;
- The unauthorized sharing of NIST-owned software or any other NIST information not authorized for disclosure or use by others with anyone not specifically authorized to receive such software or information.
- Failure to follow NIST guidelines for downloading and installing software.

Privacy of Information

NIST systems and any information on those systems are Government property. Therefore, users of NIST systems should be aware that information transmitted by or stored on NIST systems is not private. In addition, NIST users should also be

aware that it is often necessary to monitor network traffic or computer activity to ensure integrity, security or reliable operation of NIST systems. However, any other monitoring is against NIST policy. Casual reading of e-mail messages addressed to others is prohibited.

Enforcement

Unauthorized or improper use of NIST IT resources by Commerce employees is punishable by penalties as provided in the Department's Table of Offenses and Penalties (http://www.osec.doc.gov/opog/dmp/daos/dao202_751.html), which are incorporated into the NIST Administrative Manual as Appendix A to Subchapter 10.11, Adverse Actions. Unauthorized or improper use by contractors, guest researchers, collaborators, and other associates, will result in notifications to their management and NIST sponsor and can result in similar penalties and possible termination of agreements with NIST. Individuals involved with misuse will also be subject to having all computer account access indefinitely suspended at the discretion of NIST management and the NIST CIO.

Created July 06, 2009, Updated August 25, 2016