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 actions, and 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 for which a 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 any NIST user, 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 or accessing information on a system for which the user is not authorized;

• Deliberate unauthorized destruction of NIST data or other unauthorized modification of NIST data or other unauthorized modification of NIST systems;

• Commercial or business use that constitutes fraud or any other fraudulent activity.

Privacy of Information

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:

(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.

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 accessible. Information stored on or transmitted by NIST systems is not private. In addition, NIST systems are not designed to provide automated front-ending or other protection services.

Enforcement

The NIST Office of the General Counsel can be reached via e-mail at ogc@nist.gov. The Unacceptable Use of NIST Information Technology Resources code of conduct is enforced by the NIST Office of the CIO. NIST employees are held to the highest standards of integrity and professionalism. Any violations of the NIST code of conduct will be investigated and disciplinary action may be taken.

October 2003

Policy on Access and Use

NIST systems and networks are open for public access and use. Any person who accesses NIST systems and networks does so at his or her own risk. NIST does not guarantee the accuracy, reliability, or completeness of information obtained from NIST systems and networks. NIST expressly disclaims any liability, whether direct or indirect, arising from the use of NIST systems and networks.

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, which can be found on the NIST intranet. NIST employees agree to conduct themselves professionally and to refrain from using NIST resources for activities that are offensive to coworkers or the public. NIST employees further agree to conduct themselves professionally and to refrain from using NIST resources for activities that are offensive to coworkers or the public.

Privacy of Information

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:

(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.

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 accessible. Information stored on or transmitted by NIST systems is not private. In addition, NIST systems are not designed to provide automated front-ending or other protection services.

Enforcement

The NIST Office of the General Counsel can be reached via e-mail at ogc@nist.gov. The Unacceptable Use of NIST Information Technology Resources code of conduct is enforced by the NIST Office of the CIO. NIST employees are held to the highest standards of integrity and professionalism. Any violations of the NIST code of conduct will be investigated and disciplinary action may be taken.

October 2003

Policy on Access and Use

NIST systems and networks are open for public access and use. Any person who accesses NIST systems and networks does so at his or her own risk. NIST does not guarantee the accuracy, reliability, or completeness of information obtained from NIST systems and networks. NIST expressly disclaims any liability, whether direct or indirect, arising from the use of NIST systems and networks.

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, which can be found on the NIST intranet. NIST employees agree to conduct themselves professionally and to refrain from using NIST resources for activities that are offensive to coworkers or the public. NIST employees further agree to conduct themselves professionally and to refrain from using NIST resources for activities that are offensive to coworkers or 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 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 the software is distributed, or disseminated in accordance with U.S. copyright regulations, the license for that software, and NIST security policies;
- Participating 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 introducing potential vulnerabilities. NIST employees 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 obtain the name of the author or company and contact them to ask about the software.
- 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 downlaoded 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... 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 computing facilities 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 is prohibited, and is a violation of NIST information technology policy. 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 communicate access to the public, exceeds authorized access is subject to the same penalties as other unacceptable uses as described in this policy.

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 support NIST information technology resources:

- Support NIST work and projects of NIST management.
- Use NIST resources in support of NIST work and projects.
- Contribute to the NIST mission and the public good.
- Comply with NIST policies and procedures.
- Respect NIST resources, including computers, networks, and peripheral devices.
- Contribute to the NIST mission and the public good.