

Access and Use of Information Technology Resources



October 2016

The purpose of this directive is to define requirements for access and use of NIST IT resources based on requirements as stated in the Commerce Information Technology Requirements (CITR-022) Access and Use Policy.

BACKGROUND

As stated in the Commerce Information Technology Requirement (CITR-022), the DOC promotes job creation, economic growth, sustainable development, and improved standards of living for all Americans by working in partnership with businesses, universities, communities, and our nation's workers. Information is at the core of this mission, and thus other than its personnel and customers, DOC considers information as one of its most valuable assets. Technology has enabled DOC to create efficiencies in its work and has become an imperative tool in the operation and conduct of work and to the services provided to its customers.

REQUIREMENTS

Requirements defined herein are taken directly from the CITR-022, Access and Use Policy. Supplemental, issue-specific NIST rules are contained in a series of Notices titled, Access and Use. NIST information system users must report IT incidents by contacting the Information Technology Assistance Center (iTAC) (301-975-5375 or 303-497-5375 or itac@nist.gov).

1. Department of Commerce (DOC) information and IT resources may be used in the conduct of mission-related work, in the administration and management of DOC programs, and in the dissemination of the results of DOC work. The general criteria used in deciding acceptable access and use are based on general ethical principles of conduct, as well as government policies and statutory requirements.
2. DOC permits limited personal use of its information and IT resources, including telecommunication services, provided that such access complies with the requirements defined herein, does not interfere with DOC work and individual duties, and does not increase costs to the government or to the DOC. Such limited personal access and use is a privilege, not a right, and is by no means universal among Federal agencies.
3. Employees and associates are expected to conduct themselves professionally in the workplace and refrain from using information and IT resources, including telecommunications services, for activities that are not authorized under existing laws, regulations, or DOC policies. Unacceptable and prohibited uses of DOC IT resources, systems, and networks include, but are not limited to:
 - a. Use of electronic devices, systems or services for the following:

- i. Unauthorized physical or wireless connection of unapproved IT devices to internal DOC IT resources (e.g., the connection of personal smart phones or cameras for purposes of charging the battery source or accessing information, or the connection and use of personal flash drives or personal removable hard drives);
 - ii. Unauthorized use of non-DOC contracted cloud services to store DOC information;
 - iii. Electronic transmission of unencrypted sensitive information (e.g., PII) across the Internet;
 - iv. Unauthorized remote access services or mechanisms designed to bypass authorized remote access services;
 - v. Use of personally owned mobile devices and media to store sensitive DOC information;
 - vi. Unauthorized forwarding or synchronization of email or other internal DOC information or records to personally owned devices or resources;
 - vii. Installation of software on DOC IT resources that is not work-related or that has been explicitly prohibited;
 - viii. Access to any network or system for which the person has not been authorized, or in a manner that knowingly violates DOC policies;
 - ix. Unauthorized use of a system for which the user has authorized access (e.g., accessing information not needed to conduct one's official duties, or unauthorized use of privileged commands). For example, no user may access the root account on a Unix system or attempt to access the most privileged accounts on the system unless he or she is authorized and has a reason to do so; and
 - x. Sharing individual authentication credentials (e.g., smartcard, token, authenticator, PINs, passwords, etc.) with users for whom access to those credentials is not explicitly authorized.
- b. Use of DOC IT resources to conduct or participate in unethical or illegal activities:
- i. The intentional creation, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials;
 - ii. The intentional creation, downloading, viewing, storage, copying, or transmission of materials related to gambling, illegal weapons, terrorist activities, and any other illegal or otherwise prohibited activities;
 - iii. The intentional unauthorized acquisition, use, reproduction, transmission, or distribution of any DOC or OU-defined controlled information including, but not limited to, software and information that includes privacy information, copyrighted, trademarked, or otherwise protected intellectual property (beyond fair use), proprietary data, or export controlled software or data;

APPLICABILITY

- This directive applies to all NIST employees, contractors and other associates (to include non-employee students, post-docs, guest researchers, etc.), regardless of whether information technology (IT) accounts are assigned, or credentials issued; and
- All access to DOC information and IT resources, regardless of the device, network, infrastructure, or location (e.g., remote connection to a DOC network). Network access to information and services may include wired, wireless, or remote, and may include domestic or foreign destinations. Regardless of the infrastructure used to access DOC information and IT resources, access and use rules defined herein apply.

- iv. Activities which are inappropriate or offensive to fellow employees, associates, or the public. Such activities include: harassment, hate speech, or material that discriminates against others on the basis of race, creed, religion, color, age, gender, disability, national origin, or sexual orientation;
 - v. The use of government IT resources for unauthorized commercial purposes, “for-profit” activities for an individual or company, or other outside employment or business activity (such as consulting for pay, sales or administration of business transactions, sale of goods or services); and
 - vi. Engaging in any unauthorized fundraising activity, including non-profit activities, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.
- c. Inappropriate use of DOC IT resources:
- i. Unauthorized dissemination of non-public DOC information to external parties or entities that are not authorized to view them, such as newsgroups, bulletin boards, or other public forums;
 - ii. Use or creation of personal or otherwise unauthorized list servers;
 - iii. Establishing personal, commercial, and/or non-profit organizational web pages on government owned or operated information systems;

- iv. Unauthorized creation, copying, transmission, or retransmission of chain letters, unauthorized newsletters, or other unauthorized mass mailings regardless of the subject matter.
- d. Exceeding information transfer thresholds for DOC IT resources, which could cause congestion, delay, or disruption of service to the legitimate activities of anyone using DOC IT resources. For example, excessive (in proportion to resources) media streaming, or sending or downloading of excessively large file attachments can degrade the performance of the entire network.
- 4. Official DOC work and digital communications (e.g., email) must be carried out using authorized DOC IT accounts. Official DOC communications are defined as any transfer of signs, writing, images, data, or intelligence for the purpose of supporting a DOC mission or objective. Use of personal accounts for official work or communications is prohibited. There may be circumstances that warrant deviations (e.g., where there is an imminent risk to life or property, an official communication related to an emergency may be made through the use of personal email).
- 5. Records and information must be retained if:
 - a. Regulation or statute requires their retention;
 - b. Management determines they are likely to be needed for investigation or prosecution of unauthorized, illegal, or abusive acts;
 - c. Management determines they are likely to be needed in the future.
- 6. Electronic records are required to be maintained in accordance with a National Archives and Records Administration (NARA) approved record schedule, and appropriate backups maintained and tested.
- 7. Employees and associates shall not destroy or dispose of the DOC's records or information without advance management approval. The use of social media may create Federal records that must be captured and managed in compliance with Federal records management laws, regulations, and policies.
- 8. Routine continuous monitoring of networks and IT systems is conducted to identify and respond to performance-degrading events such as equipment failures, capacity issues, security threats, and security breaches. Therefore, all employees and associates using DOC systems should be aware that information transmitted by or stored on systems within DOC's purview is not private.
- 9. While in official duty status, employees may not use technology to secretly overhear, transmit, or record communications. In lieu of a reporter or secretary taking verbatim transcriptions or notes of conferences or meetings, conventional conference equipment may be utilized, provided that advance notice is given to, and approval obtained from

the participants in the conference or meeting.

10. Personal photography is generally authorized without prior permission, however, photography of sensitive areas, equipment, or documentation is prohibited. Further, DOC policy requires mutual consent to photograph or record guest speakers, officials or activities.
11. All DOC employees and associates must promptly report incidents involving information and information technology resources. Incidents may include suspected or confirmed presence of malware, policy violations, misuse, loss or breach of PII, loss or theft of a smartcard, smartphone, laptop, tablet, etc. Further, employees and associates may not impede actions taken to conduct a forensic evaluation and/or sanitize information technology resources. DOC management has an even greater responsibility to report and remediate incidents as soon as they are observed and/or reported to them so as to reduce the risk and liability to the DOC.
12. Unacceptable access and/or use of DOC information and information technology resources by employees may subject the employee(s) to discipline in accordance with existing DOC policy, including the penalties provided in Department Administrative Order (DAO) 202-751, Discipline (see reference in Section 7).
13. Unacceptable access and/or use by contractors or other associates will result in notifications to the host organization management and may result in similar penalties and possible termination of agreement to work with DOC.
14. Employees, contractors or other associates engaging in unacceptable access and/or use shall also be subject to having all IT accounts and/or other credentials indefinitely suspended at the discretion of DOC and/or OU management and the Departmental and/or OU Chief Information Officer.

RESPONSIBILITIES

Office of Information Systems Management

- Enforces formal acknowledgment of Access and Use rules.

NIST Supervisors

- Ensures compliance with Access and Use rules.

Information System Users

- Reads, understands, acknowledges, and adheres to this Order and supplemental Access and Use Notices.