National Weather Service (NWS)

Configuration Branch Information Technology Systems (CBITS)

FISMA ID: NOAA8100

Rules of Behavior

November 7, 2017

Record of Changes/Revisions

This is a living document that is changed as required to reflect system, operational, or organizational changes. Modifications are recorded in the Change/Revision Record below. This record shall be maintained throughout the life of the document.

Change / Revision Record			
DATE	SECTION	DESCRIPTION OF CHANGE	MADE BY
12/2006	All	Version 1.0 No Prior Documents Exist	Michelle Detommaso
2/2/2009	All	Version 2 – Updated for FY2009 C&A	Michelle Detommaso
11/7/2017	All	Version 3 – Updated to CITR-022 language and to include the NOAA Privacy Act Statement	Brady Malone

INTRODUCTION

The Configuration Branch Information Technology Systems (NOAA8100-CBITS) employs existing NOAA guidance as its mechanism to assure all users act in accordance with NOAA policies.

NOAA8100-CBITS uses NOAA email account and passwords, and therefore leverages NOAA guidance for its Rules of Behavior (Access and Use Policy), as defined by CITR-022. There are no additional Rules of Behavior applicable for NOAA8100-CBITS. NOAA8100-CBITS authenticates users via NOAA LDAP as directed by NWS Regional Management. Utilizing CITR-022, no additional NWS Employee Union clearance is needed. For user reference, CITR-022 is included below.

NOAA8100-CBITS users shall acknowledge and accept the NOAA Privacy Act Statement regarding the storage of user ID, work email addresses and work telephone numbers. The statement is included below for user reference.

Privacy Act Statement

Authority: The collection of this information is authorized under 5 U.S.C. § 301, Departmental regulations.

Purpose: The Department of Commerce (Department) is collecting this information to ensure that NOAA staff and contractors have the most current contact information available so that other staff may contact them when needed.

Routine Uses: The Department will use this information to maintain an accurate contact list for NOAA staff and contractors for daily work purposes. Disclosure of this information is permitted under the Privacy Act of 1974 (5 U.S.C. Section 552a**)** to be shared among Department staff for work-related purposes. Disclosure of this information is also subject to all of the published routine uses as identified in the Privacy Act System of Records Notice COMMERCE/DEPT-18, Employees Personnel Files Not Covered by Notices of Other Agencies.

Disclosure: Furnishing this information is voluntary; however, failure to provide accurate information may delay or prevent the individual from being contracted when needed in the context of work.

Department of Commerce
Commerce Information Technology Requirement
Access and Use Policy
CITR-022
April 15, 2014

1. PURPOSE

This document establishes requirements for access to and use of U.S. Department of Commerce (DOC) information and technological resources.

2. BACKGROUND

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.

Given that information is an asset, DOC strives to protect the confidentiality, integrity, and availability of its information and technological resources, and thus imposes a baseline security categorization on all its information. This means that all non-public DOC information requires at least minimum security controls (i.e., low) to protect it. Some of this information, such as personally identifiable information (PII), financial , or other types of information which requires protection from unauthorized disclosure, require more stringent security controls (e.g., use of encryption) . This more sensitive information must be protected using at least a moderate level of security. While automated means are in place to enhance security, each DOC user of information and associated technology has a duty to protect information at its defined level.

3. SCOPE

Requirements defined herein apply to:

- All DOC 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.

4. AUTHORITY

The DOC Chief Information Officer (CIO) has the authority to develop, implement, and manage IT security processes and procedures to protect the availability, confidentiality, and integrity of the DOC's IT resources. The DOC Chief Information Security Officer (CISO)/Senior Agency Information Security Officer (SAISO) shall ensure that IT security policy and requirements are developed consistent with applicable statutory authority, including the Clinger-Cohen Act and Federal Information Security Management Act (FISMA); with regulatory requirements and external guidance, including Office of Management and Budget (0MB) policy and Federal Information Processing Standards (FIPS) publications promulgated by the National Institute of Standards and Technology (NIST); and with internal policies and requirement s.

5. CANCELLATION/AUGMENTATION OF EXISTING POLICY

This policy replaces the DOC Internet Use Policy and the Personal Email for Official Communication Prohibited IT Security Policy memo, and augments the DOC Telecommunications Management Policy.

6. POLICY

6.1. Baseline Requirements

This policy establishes baseline requirements for Access and Use. DOC Operating Units (OUs) may establish more restrictive requirements based on their unique mission, sensitivity of their information, existing labor management agreements, or the capabilities of the supporting infrastructure. OUs may establish processes for reviewing and adjudicating exceptions to this policy, or to their own, more restrictive Access and Use policy. Nothing in this policy shall abrogate or override any Collective Bargaining Agreement in effect on the date this policy is issued.

6.2. Acknowledgment of Access and Use Policy

CIOs of all OUs that provide IT services shall ensure written acknowledgment of the Department or locally-derived Access and Use Policy prior to granting access to any non-public IT systems, networks, or resources. This may be accomplished by providing employees and associates with a copy of this policy and obtaining a written acknowledgment that they have read and understood the policy, or by developing a separate access and use form that describes this policy, to be signed by an employee or associate prior to that individual being provided access to IT systems/network/ resources.

6.3. Acceptable Access and Use

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.

6.4. Limited Personal Access and Use

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.

6.5. Unacceptable Access and Use

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:

1) Use of electronic devices, systems, or services for the following:

   a) 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 for accessing information, or the connection and use of personal flash drives or personal removable hard drives);
   b) Unauthorized use of non-DOC contracted cloud services to store DOC information;
   c) Electronic transmission of unencrypted sensitive information (e.g., PII) across the Internet;
   d) Unauthorized remote access services or mechanisms designed to bypass authorized remote access services;
   e) Use of personally owned mobile devices and media to store sensitive DOC information;
   f) Unauthorized forwarding or synchronization of email or other internal DOC information or records to personally owned devices or resources;
   g) Installation of software on DOC IT resources that is not work-related or that has been explicitly prohibited;
   h) Access to any network or system for which the person has not been authorized, or in a manner that knowingly violates DOC policies;
   i) 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;

j) Sharing individual authentication credentials (e.g., smartcard, token, authenticator, PINs, passwords, etc.) with users for whom access to those credentials is not explicitly authorized.

2) Use of DOC IT resources to conduct or participate in unethical or illegal activities:
   a) The intentional creation, downloading, viewing, storage, copying, or transmission of sexually explicit or sexually oriented materials;
   b) 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;
   c) 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;
   d) 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;
   e) 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);
   f) 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.
3) Inappropriate use of DOC IT resources:
   a) 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;
   b) Use or creation of personal or otherwise unauthorized list servers ;
   c) Establishing personal, commercial, and/or non-profit organizational web pages on government owned or operated information systems;
   d) Unauthorized creation, copying, transmission, or retransmission of chain letters, unauthorized newsletters, or other unauthorized mass mailings regardless of the subject matter.
4) 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 available resources) media streaming, or sending or downloading of excessively large file attachments can degrade the performance of the entire network.

6.6. Official work, communications, and records

Official DOC work and digital communications (e.g., email) must be carried out using

authorized DOC IT accounts. Official DOC communication s 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 e-mail).

Records and information must be retained if: (1) regulation or statute requires their retention; (2) management determines they are likely to be needed for investigation or prosecution of unauthorized, illegal, or abusive acts; or (3) management determines they are likely to be needed in the future. 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. 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.

6.7. Privacy

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 threat s, and security breaches. Therefore, all employees and associate s using DOC systems should be aware that information transmitted by or stored on systems within the DOC's purview is not private.

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 conference s 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.

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.

6.8. Incident Reporting and Handling

All DOC employees and associates shall 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 smart card, smartphone , laptop, tablet, etc. Further, employees and associates may not impede action s 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 risk and liability to the DOC.

6.9. Enforcement

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 Sec. 7). 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 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.

6.10. Updates

Supplemental requirements may be issued by each DOC OU as their environment dictates.

6.11. Information and Assistance

Questions or comments shall be directed to the appropriate DOC OU Chief Information Officer and/or central service desk.

6.12. Effective Date

CITR-022 is effective as of July 15th, 2014.