Homeland Security

DHS 4300A Sensitive Systems Handbook

Attachment G

Rules of Behavior

Version 11.0

August 5, 2014

Protecting the Information that Secures the Homeland

This page intentionally blank

Document Change History

Version	Date	Description
1.0	April 25, 2003	Initial release
1.1	February 9, 2004	Revised document title
2.0	March 31, 2004	Content updated
3.0	April 30, 2005	General rules of behavior and the rules of behavior for laptops and portable electronic devices were combined; information on developing system-specific rules of behavior was added.
3.1	July 29, 2005	Minor editorial change
4.0	June 1, 2006	Addition of password-protection rules; addition of two Internet and email usage rules.
5.0	March 1, 2007	Addition/modification of rules for passwords and for laptop computers/portable electronic devices.
6.0	May 14, 2008	No change.
6.1	September 23, 2008	Addition of rules regarding limitations of Internet activities, webmail or other personal email accounts, and offensive content.
7.0	August 7, 2009	Updated reference to 140-1 Management Directive
9.1	July 24, 2012	Stylistic changes, grammar and diction.
11.0	August 5, 2014	Removed term “PED,” changed to “mobile computing and communication devices.”

CONTENTS

1.0 GENERAL RULES OF BEHAVIOR

Rules of behavior that apply to access and use of Department of Homeland Security (DHS) information technology (IT) equipment and systems are a vital part of the DHS IT Security Program, and help to ensure the security of systems and the confidentiality, integrity, and availability of sensitive information.

The purpose of DHS Rules of Behavior is to inform users of their responsibilities and let them know they will be held accountable for their actions while they are accessing DHS systems and using DHS IT resources capable of accessing, storing, receiving, or transmitting sensitive information. The DHS Rules of Behavior apply to every DHS employee and DHS support contractor.

Attached are the baseline rules of behavior that apply to all users of DHS systems and IT devices capable of accessing, storing, receiving, or transmitting sensitive information. These Rules of Behavior are consistent with the IT security policy and procedures given by DHS Management Directive 140-1, "Information Technology Systems Security", "DHS Sensitive Systems Policy Directive 4300A," and the "DHS 4300A Sensitive Systems Handbook." Components can tailor these Rules of Behavior to apply to their own systems and IT devices; they may establish more stringent rules than those attached, but may neither remove nor make less stringent any rule attached hereto.

Where users are not subject to Component-specific rule(s) of behavior, they must comply with those published by the Department. Any user not in compliance with applicable Rules of Behavior is subject to sanctions that may include verbal or written warning, denial of system access for a specific period of time, reassignment to other duties, criminal or civil prosecution, or termination, depending on the severity of the violation.

2.0 SYSTEM-SPECIFIC RULES OF BEHAVIOR

In addition to having to read, accept, and sign the general Rules of Behavior that apply to DHS systems and IT resources, users also are required to read, accept, and sign Rules of Behavior that apply specifically to systems to which they will have access. Components are responsible for developing such Rules of Behavior and for having users read and sign them.

Appendix III to OMB Circular A-130, "Management of Federal Information Resources," and NIST Special Publication (SP) 800-18, Rev. 1, "Guide for Developing Security Plans for Federal Information Systems" provide requirements for system-specific rules of behavior for general support systems (GSS) such as local area networks (LAN) and for major applications (MA). These requirements include the following:

- Rules of behavior shall be in writing.
- The rules shall delineate responsibilities and expected behavior of all individuals with access to the system and shall state the consequences of behavior not consistent with the rules.

- The rules shall cover such matters as teleworking, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of Government equipment, assignment and limitation of system privileges, and individual accountability.
- The rules shall state appropriate limits on interconnections to other systems and shall define service provision and restoration priorities.
- The rules shall reflect technical security controls (e.g., rules regarding passwords should be consistent with technical password features).
- The rules shall include limitations on changing data, searching databases, or divulging information.
- The rules shall state that controls are in place to ensure individual accountability and separation of duties and to limit the processing privileges of individuals.
- Users shall read and sign rules of behavior before they are given to Government systems.

Section 1.8 of NIST SP 800-18, Rev. 1, "Guide for Developing Security Plans for Federal Information Systems," provides example rules of behavior.

The Information Systems Security Officer (ISSO) shall ensure that a user reads, accepts, and signs the general rules of behavior and all system-specific rules of behavior pertaining to systems to which that user will be given access; the rules must be signed before the user is given access. The signed rules of behavior may be filed either in the employee's Official Personnel Folder (OPF) or in the employee's personnel file

General Rules of Behavior for Users of DHS Systems and IT Resources that Access, Store, Receive, or Transmit Sensitive Information

The following rules of behavior apply to all Department of Homeland Security (DHS) employees and support contractors who use DHS systems and IT resources including workstations, laptop computers, and mobile computing devices (including cell phones, smartphones, tablets, removable media such as CDs, DVDs, and both mechanical and solid state portable memory drives) to access, store, receive, or transmit sensitive information. ,

These rules of behavior are consistent with the IT security policy and procedures given in DHS Management Directive 140-1, "Information Technology Systems Security, DHS Rules of Behabior apply to users at their primary workplace while teleworking or at a satellite ssite, and at any These rules of behavior are consistent with the IT security policy and procedures given in DHS Management Directive 140-1, "Information Technology Systems Security," DHS Sensitive Systems Policy Directive 4300A, and the DHS 4300A Sensitive Systems Handbook.

DHS Rules of Behavior apply to users at their primary workplace, while teleworking or at a satellite site, at any alternative workplaces, and while traveling.

System Access

- I understand that I am given access only to those systems to which I require access in the performance of my official duties.
- I will not attempt to access systems I am not authorized to access.

Passwords and Other Access Control Measures

- I will choose passwords that are at least eight characters in length and include upper and lower case letters, numerals, and special characters. I will protect passwords and access numbers from disclosure. I will not share passwords. I will not provide my password to anyone, including system administrators. I will not record passwords or access control numbers on paper or in electronic form, and I will not store them on or with DHS workstations, laptop computers, or mobile computing devices. To prevent others from obtaining my password via "shoulder surfing," I will shield my keyboard from view as I enter my password.
- I will ensure that my Personal Identity Verification (PIV) card is always in my personal possession.
- I will not record or transmit my Personal Identification Number (PIN)
- I will not store my PIV card with with DHS workstations, laptop computers, or mobile computing devices.

- I will promptly change a password whenever its compromise is known or suspected to have occurred.

- I will not attempt to bypass access control measures.

Data Protection

- I will use only DHS equipment, and never personally owned equipment, to access DHS systems and information.

- I will protect sensitive information from disclosure to unauthorized persons or groups.

- I will log off or lock my workstation or laptop computer, or I will use a password-protected screensaver, whenever I am away from my work area, even for a short time; I will log off when I leave for the day.

- I will not access, process, or store classified information on DHS office equipment that has not been authorized for classified information of commensurate level.

Use of Government Office Equipment

- I will comply with DHS policy regarding personal use of DHS office equipment. I understand that DHS office equipment is to be used for official purposes, with only limited personal use allowed. Personal use of Government office equipment is described in DHS Management Directive (MD) 4600, "Personal Use of Government Office Equipment."

- I understand that my use of DHS office equipment may be monitored, and I consent to this monitoring.

- I understand that only OPA-designated content managers may post material to Department and Component Internet sites.

- I understand that Internet activities which inhibit the security of DHS information and information systems, or cause degradation of network services are prohibited. Examples of such activity include streaming of audio or video, social networking, peer-to-peer networking, software or music piracy, online gaming, webmail, Instant Messaging (IM), and hacking.

- I understand that the use of webmail or other personal email accounts is prohibited on DHS information systems.

- I understand that the viewing of pornographic or other offensive content is strictly prohibited on DHS furnished equipment and networks.

Software

- I agree to abide by software copyrights and to comply with the terms of all licenses.

- I will not install on DHS equipment unauthorized software, including software available for downloading from the Internet, software available on DHS networks, and personally owned software

Internet and Email Use

- I understand that I can only use Government systems for official Internet activities and email, with limited personal use allowed. Allowed personal use is described in DHS MD 4500, "DHS E-mail Usage" and DHS MD 4400.1, "DHS Web and Information Systems."

- I will not use Government systems for access to webmail.

- I understand that my Internet and email use may be monitored, and I consent to such monitoring.

- I will not use peer-to-peer (P2P) file sharing to connect remotely to other systems for the purpose of sharing files. I understand that P2P can be a means of spreading viruses over DHS networks and may put sensitive government information at risk. I also understand that DHS Sensitive Systems Policy Directive 4300A prohibits the use of P2P software on any DHS-controlled or DHS-operated system.

- I will not provide personal or official DHS information if solicited by email. I f I receive email from any source requesting personal or organizational information. If I receive an email message from any source requesting personal information or asking to verify accounts or security settings, I will send the questionable email to the purported source company for verification and I will report the incident to the DHS Help Desk.

Teleworking

Employees approved for teleworking at any alternate workplace must adhere to the following additional rules of behavior:

- At my alternate workplace, I will follow security practices that are the same as or equivalent to those required of me at my primary workplace.

- I will physically protect any communications and computing equipment I use for teleworking when they are not in use.

- I will protect sensitive data at my alternate workplace. This includes disposing of sensitive information by shredding or other appropriate means.

Laptop Computers and Portable Electronic Devices

Use of DHS communications and computing devices is subject following additional rules of behavior:

- I will use only DHS communications and computing devices to access DHS systems and information.

- I will password-protect any communications and computing devices I use. I will set the security timeout for any communications and computing device to the established timeout period. For GFE communications and comput8ing devices, the timeout period is 10 minutes.

- I will keep Government furnished equipment under my physical control at all times, or I will secure it in a suitable locked container under my control.

- I will take all necessary precautions to protect Government furnished equipment against loss, theft, damage, abuse, and unauthorized use by employing lockable cases and keyboards, locking cables, and removable storage devices.

- I will immediately comply with instructions from technical support personnel to perform update actions, or to make equipment assigned to me available to technical support personnel for updating.

- I will use only DHS-authorized Internet connections that conform to DHS security and communications standards.

- I will not make any changes to a laptop's system configuration unless I am directed to do so by a DHS system administrator.

- I will not program the laptop with sign-on sequences, passwords, or access phone numbers.

- I understand and will comply with the requirement that sensitive information stored on any laptop computer used in a residence or on travel shall be protected using encryption validated in accordance with FIPS 140-2, "Security Requirements for Cryptographic Modules."

- I understand and will comply with the requirement that sensitive information processed, stored, or transmitted on wireless devices must be encrypted using approved encryption methods.

Incident Reporting

- I will promptly report IT security incidents in accordance with DHS CISO procedures for detecting, reporting, and responding to information security incidents in accordance with *DHS 4300A Sensitive Systems Handbook*, Attachment F, "Incident Reporting."

Accountability

- I understand that I have no expectation of privacy while using any DHS equipment and while using DHS Internet or email services.
- I understand that I will be held accountable for my actions while accessing and using DHS systems and IT resources.

Acknowledgment Statement

I acknowledge that I have read, understand, and will comply with the DHS Rules of Behavior. I understand that failure to comply with the Rules of Behavior could result in one or more of the following actions: verbal or written warning; removal of system access; reassignment to other duties; criminal or civil prosecution; termination.

Name of User (printed): _____

User's Phone Number: _____

User's Email Address: _____

DHS Component: _____

Location or Address: _____

Supervisor: _____

Supervisor's Phone Number: _____

_____ _____

User's Signature Date

Tips for Traveling with a Mobile Computing Device

Keep the mobile computing device under your physical control at all times.

At airport security, place the mobile computing device on the conveyor belt only after the belongings of the person ahead of you have cleared the scanner. If you are delayed, keep your eye on the mobile computing device until you can pick it up.

Do not place the mobile computing device in checked luggage.

Do not store or check the mobile computing device in an airport, a train or bus station, or any public locker.

If you must leave a mobile computing device in a car, lock it in the trunk so that it is out of sight.

Avoid leaving a mobile computing device in a hotel room. If you must leave it in a hotel room, lock it inside another piece of luggage.