Attachment G

Rules of Behavior

DHS 4300A
Sensitive Systems Handbook

Version 5.0

March 1, 2007

DEPARTMENT OF HOMELAND SECURITY

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 e-mail usage rules.
5.0	March 1, 2007	Addition/modification of rules for passwords and for laptop computers/portable electronic devices.

CONTENTS

1.0 GENERAL RULES OF BEHAVIOR

Rules of behavior regarding the access of Department of Homeland Security (DHS) systems and the use of its IT resources are a vital part of the DHS IT Security Program. Rules of behavior that are understood and followed help ensure the security of systems and the confidentiality, integrity, and availability of sensitive information. Rules of behavior 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 DHS employees and to DHS support contractors.

Attached are sample general 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 IT security policy and procedures within DHS Management Directive 4300.1 (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, or they can develop their own set of rules.

Any person who is in noncompliance with the rules of behavior is subject to penalties and sanctions, including verbal or written warning, removal 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 and sign the general rules of behavior regarding DHS systems and IT resources, users also are required to read and sign rules of behavior specific to those DHS 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 and NIST Special Publication 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 (e.g., local area networks) and major applications. These requirements include the following:

- Rules of behavior specific to the system 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 work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of government equipment, the 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 processing privileges of individuals.
- Users shall read and sign rules of behavior specific to the systems to which they require access before they are given that access.

NIST Special Publication 800-18, Rev. 1, *Guide for Developing Security Plans for Federal Information Systems,* provides rules of behavior examples in Section 1.8.

The Information Systems Security Officer (ISSO) shall ensure that a user reads and signs the general rules of behavior and all other system-specific rules of behavior for 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 such as laptop computers and portable electronic devices (PED) to access, store, receive, or transmit sensitive information. PEDs include personal digital assistants or PDAs (e.g., Palm Pilots), cell phones, text messaging systems (e.g., Blackberry), and plug-in and wireless peripherals that employ removable media (e.g., CDs, DVDs). PEDs also encompass USB flash memory (thumb) drives, external drives, and diskettes.

These rules of behavior are consistent with IT security policy and procedures within DHS Management Directive 4300.1 (Information Technology Systems Security), DHS Sensitive Systems Policy Directive 4300A, and the DHS 4300A Sensitive Systems Handbook.

The rules of behavior apply to users at their primary workplace and at any alternative workplaces (e.g., telecommuting from home or from a satellite site). They also apply to users on official travel.

System Access

- I understand that I am given access to only those systems for which I require access to perform 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 long and have a combination of letters (upper- and lower-case), numbers, 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 store them on or with DHS workstations, laptop computers, or PEDs. To prevent others from obtaining my password via "shoulder surfing," I will shield my keyboard from view as I enter my password.

- I will not store smart cards on or with DHS workstations, laptop computers, or PEDs.
- I will promptly change a password whenever the compromise of that password is known or suspected.
- I will not attempt to bypass access control measures.

Data Protection

- I will use only DHS office equipment (e.g., workstations, laptops, PEDs) to access DHS systems and information; I will not use personally owned equipment.
- 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 step 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 such processing.

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 use, 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.

Software

- I agree to comply with all software copyrights and licenses.
- I will not install unauthorized software (this includes software available for downloading from the Internet, software available on DHS networks, and personally owned software) on DHS equipment (e.g., DHS workstations, laptop computers, PEDs).

Internet and E-mail Use

- I understand that my Internet and e-mail use is for official use, 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 understand that my Internet and e-mail use may be monitored, and I consent to this 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 operated equipment.
- I will not provide personal or official DHS information solicited by e-mail. I will be on alert if I receive e-mail from any source requesting personal or organizational

information. If I receive an e-mail message from any source requesting personal information or asking to verify accounts or security settings, I will send the questionable e-mail to the company for verification and report the incident to the DHS Help Desk.

Telecommuting (Working at Home or at a Satellite Center)

Employees approved for telecommuting must adhere to the following 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 laptops or PEDs I use for telecommuting when they are not in use.
- I will protect sensitive data at my alternate workplace. This includes properly disposing of sensitive information (e.g., by shredding).

Laptop Computers and Portable Electronic Devices

Rules of behavior that specifically apply to DHS laptop computers and portable electronic devices (PEDs) are listed below.

- I will use only DHS laptops or PEDs to access DHS systems and information.
- I will password-protect any BlackBerry device, smartphone, or other PED. I will set the security timeout for any PED to the established timeout period. For BlackBerry devices, this timeout period is 10 minutes.
- I will keep the laptop or PED under my physical control at all times, or I will secure it in a suitable locked container under my control.

Tips for Traveling with a Laptop or PED

- Keep the laptop or PED under your physical control at all times.
- At airport security, place the laptop or PED 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 laptop or PED until you can pick it up.
- Do not place the laptop or PED in checked luggage.
- Do not store the laptop or PED in an airport, a train or bus station, or any public locker.
- If you must leave a laptop or PED in a car, lock it in the trunk so that it is out of sight.
- Avoid leaving the laptop or PED in a hotel room. If you must leave it in a hotel room, lock it inside another piece of luggage.

- I will take all necessary precautions to protect the laptop/PED against loss, theft, damage, abuse, or unauthorized use by employing lockable cases and keyboards, locking cables, and removable media drives.

- I will keep antivirus and firewall software on the laptop up to date.
- 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 encrypted using FIPS 140-2 *Security Requirements for Cryptographic Modules* approved encryption.
- 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.

Accountability

- I understand that I have no expectation of privacy while using any DHS equipment and while using DHS Internet or e-mail 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 the rules of behavior, I understand them, and I will comply with them. I understand that failure to comply with these rules could result in verbal or written warning, removal of system access, reassignment to other duties, criminal or civil prosecution, or termination.

Name of User (printed): _____

User's Phone Number: _____

User's E-mail Address: _____

DHS Component: _____

Location or Address: _____

Supervisor: _____

Supervisor's Phone Number: _____

_____ _____

User's Signature Date