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, Other government Agency (OGA) 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, cell phones, removable media such as CDs, DVDs, and both mechanical and solid state portable memory drives.

These rules of behavior are consistent with 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 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 a Personal Identity Verification (PIV) card with DHS workstations, laptop computers, or PEDs.
- 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 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 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 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 E-mail Use

- I understand that I can only use Government systems for official Internet activities and email, with limited 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 equipment.
- I will not provide personal or official DHS information if solicited by email. If I receive an email message from any source requesting 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 laptops or PEDs 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 laptop computers and portable electronic devices (PEDs) is subject to the following additional rules of behavior:

- I will use only DHS laptops or PEDs to access DHS systems and information.
- I will password-protect any PED I use. I will set the security timeout for any PED to the established timeout period. For Government cellular telephones, 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 keep antivirus and firewall software on the laptop up to date.
- I will use only DHS-authorized Interned 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.

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 or check 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 a laptop or PED in a hotel room. If you must leave it in a hotel room, lock it inside another piece of luggage.

- 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. Incidents will be reported to the DHS/ICE Service Desk at 888-347-7762, or if able to logon, you may request assistance online at https://servicedesk.ice.dhs.gov/servicedesk/

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. Additionally, I verify that I have taken the annual ICE Information Assurance Awareness Training or equivalent Computer Security Training. I understand that failure to comply with the Rules of Behavior 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): _____

PICS User ID (if applicable): _____

User's Phone Number: _____

User's Email Address: _____

Agency/ Department or Company Name: _____

Contractor Company Name: _____

Location or Address: _____

Supervisor: _____

Supervisor's Phone Number: _____

_____ _____

User's Signature Date

Filing:

Original - On site ISSO

Copy – ICE-OCIO-PICS/IRCA Manager

Copy - Individual