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 (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 allowed 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 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.
- When applicable, 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

- If applicable, 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).
- If applicable, I understand that my Internet and e-mail use may be monitored, and I consent to this monitoring.

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 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): _____

PICS User ID (if applicable): _____

User's Phone Number: _____

User's E-mail Address: _____

Agency/ Department or Company Name: _____

Contractor Company Name: _____

Location or Address: _____

Supervisor: _____

Supervisor's Phone Number: _____

_____ _____

Signature Date

Filing:

Original - On site ISSO

Copy – ICE-OCIO-PICS/IRCA Manager

Copy - Individual