Attachment A
to
Appendix C ACE Systems Security

Rules of Behavior

From Attachment G of the
DHS 4300A
Sensitive Systems Handbook
Revised for Participating Government Agency Users of ACE
Modified 4/29/08

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

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 PGA resources accessing, storing, receiving, or transmitting sensitive information. These DHS rules of behavior apply to Participating Government Agency (PGA) employees who access the CBP Automated Commercial Environment System.

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.

The following rules of behavior apply to all Participating Government Agency employees accessing the CBP ACE system. ACE data is sensitive and should be safeguarded appropriately.

Should there be inconsistency between the DHS Rules of Behavior and those governing the Participating Government Agency, the more rigorous or stringent rule will apply.

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 record passwords or access control numbers on paper or in electronic form and store them on or with 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 PGA equipment or with 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 PGA office equipment (e.g., workstations, laptops, PEDs) to access the ACE system and its 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.

Use of Government Office Equipment

- I will comply with DHS and PGA rules regarding the use of PGA office equipment for personal use.

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 PGA equipment used to access ACE.

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 PGA laptop computers and portable electronic devices (PEDs) are listed below.

- I will use only PGA laptops or PEDs to access ACE.
- 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.
- 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 PGA-authorized Internet connections that conform to DHS/PGA security and communications standards.
- I will not make any changes to a laptop's system configuration unless I am directed to do so by my PGA 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 140-1- or FIPS 140-2-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 accessing ACE.
- I understand that I will be held accountable for my actions while accessing and using ACE.

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, criminal or civil prosecution, or termination.

Name of User (printed): _____

User's Phone Number: _____

User's E-mail Address: _____

Agency: _____

Location or Address: _____

Supervisor: _____

Supervisor's Phone Number: _____

_____ _____

User's Signature Date

The PGA Systems Security Officer (SCO) shall ensure that a user reads and signs these rules of behavior for the ACE 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 in either the employee's Official Personnel Folder (OPF) or in the employee's personnel file.

ACRONYMS RELEVANT TO THIS DOCUMENT

- CBP Customs and Border Protection
- ACE Automated Commercial Environment
- PGA Participating Government Agency