U.S. Customs and Border Protection

Attachment X

Access Control Procedures

HB 1400-05D
Information Systems Security Policies and Procedures Handbook

Version 2.0

July 27, 2009

DOCUMENT CHANGE HISTORY

Version Number	Date	Description
1.0	July 27, 2009	Initial CBP 1400-05D release is based solely on existing 1400-05C, Version 2.1 appendices which were found to be unrelated to existing DHS 4300A, Version 6.1.1 attachments. The policy content of this attachment is exactly the same as the 1400-05C, Version 2.1 appendix. It is now presented in the attachment format.
2.0	December 21, 2010	No Changes

CONTENTS

1.0 Computer Access

The following practices are required of all users to decrease the chances of inadvertently exposing data to unauthorized individuals.

1. Do not connect directly or indirectly to any CBP-owned system or data network (local or wide area) with equipment that is not approved by the DAA.

2. When possible, position computer components such as monitors, displays, and printers so that unauthorized personnel cannot view the material being printed or displayed.

3. In preparation for having the OIT password-protected screen saver activated within 5 minutes of inactivity, the user should follow these steps.

   - Right click anywhere on the Desktop
   - Right click on the 'Properties' button
   - Click on the 'Screen Saver' button.
   - Use this screen to customize the screen saver, including the setting for activating the 'Password Protection' feature of the screen saver and the amount of time the workstation will sit idle before the screen saver appears. The time should be set to no more than 5 minutes to conform to policy.

4. Prevent unauthorized access to the workstation within your workspace or office by locking your workstation. On systems running Microsoft Windows simultaneously press CTRL+ALT+DEL. This will bring up a security dialog box with several option buttons. Press Enter or click Lock Workstation. To unlock your computer press CTRL+ALT+DEL, type your password, and then click OK or press Enter. This option does not terminate the applications that are running.

5. If a single user workstation is to be left unattended for more than 5 minutes, log off your LAN session. Follow the instructions in item "4." above; but click the '**Log Off'** button. This will log you off the LAN and any applications that are running. **Do activate a password-protected screen saver. Do not turn off the power.**

6. When leaving the workstation for the day, simultaneously depress the Control, Alt, and Delete keys. This enables the shutdown and restart of the workstation and will bring up a window with several option buttons. Click on the 'shutdown' button. Of the three shutdown options given, select the middle option, '**Shutdown and Restart.**' Allow the computer to restart, but do not log in. This will allow the system to load new OIT-provided software and enhancements during nights and weekends. **Do not turn off the power.**

7. If a multi-user workstation is to be left unattended for more than 30 minutes, follow the instructions in item "5." Above; but **do not activate a password-protected screen saver. Do not turn off the power.**

8. For those workstations that are operational on a 24 hours basis, the workstation must be restarted daily. To restart follow the instructions in item 7 but log in after the system reboots. This action will allow the workstation to receive new software and enhancements.

9. Whenever possible, secure unattended computer areas by locking the office doors.

10. Reading, altering, inserting, copying, browsing, searching, or deleting any data owned by CBP; participating federal; state and local governments or private businesses is prohibited, except in performance of authorized government duties.

11. Do not access government-owned data above your authorization level. This is a violation of CBP policy.

Protect information produced by any CBP system from improper disclosure. Disclosure of any CBP information is only allowed when required as part of your official duties.

2.0 Protecting Access Control Devices

Pocket-sized access control devices (e.g., lock keys, smartcards, encryption cards/keys, security codes) must be protected from loss or unauthorized access. In some cases, the loss may require replacement at both sending and receiving locations. The following security practices apply to such devices:

1. Protect any access control device in your possession at all times.

2. Keep a smartcard with its card reader and computer within your constant protection. If the smartcard and the card reader are to be left out of your control, it is recommended that the smartcard be separated from the card reader.

3. Report the loss or compromise of any lock key or encryption device immediately to your System Administrator (SA) or manager.

4. Report the loss of a smartcard to the System/LAN administrator, your manager and the CSIRC. Contact information for the CSIRC is provided in Section 5.6. A replacement device cannot be issued without an incident report on file.

3.0 Terminated and Departing Employees

1. System/LAN Administrators and managers must terminate all departing employees access privileges immediately. Under no circumstances are former employees permitted to have any ability to access system resources after their term of employment has ended. Procedures vary depending on whether the separation is voluntary of involuntary.

a. Voluntary – Terminate the employee account no later then the close of business on the last day of employment.

b. Involuntary – Terminate the employee account at the same time or prior to the employee is notified of the conclusion of his/her employment.

2. When leaving CBP, CBP employees will complete a Separation Clearance Certification Form (CF-241). Submission of this form initiates the process of revoking system access for the departing individual. The employee's supervisor must submit the CF-241 form to the OIT, TOD, Integrated Applications Security Branch to revoke the system access of the terminating employee.

3. When leaving CBP, contractors will complete the Contractor Employee Clearance Separation Form (CF-242). This form will initiate the process of revoking system access for the individual departing from CBP. Refer to CBP Directive 51715-006 for the procedure to submit the CF-242 to the OIT, TOD, Integrated Applications Security Branch in order to revoke the access of the terminating contractor.

4.0 Automatic Account Lockout

Users will be locked out from their account after three consecutive failed logon attempts during a 48 hour time period. This lockout will be for an indefinite amount of time. A system administrator will be required to reset passwords for users who have been locked out from their accounts.

When a user logs on for the first time after having his/her password reset, he/she must select a new, secure password in accordance with the requirements in Appendix D.

5.0 Automatic Session Termination

A session refers to a connection between a terminal device (workstation, laptop, PED, etc) and a networked application or system. (This does not include a direct connection to a DHS network, such as authenticating from a device that is directly connected to a DHS network.) A session also refers to accessing an application or system through the DHS network, such as a database or networked application.

Networked applications or systems shall be configured to automatically disconnect or lock any user session following 20 minutes of inactivity.

Locked sessions shall remain locked until the user re-authenticates.

Sessions shall automatically be terminated after 60 minutes of inactivity.

6.0 Automatic Mainframe Session Disconnect

CBP mainframe system shall be configured to terminate any user session immediately and automatically following 20 minutes of inactivity. The mainframe shall be configured in such a

way that will require the user to re-authenticate his identity before resuming interaction with the system. An entry will be made in the audit trail for each automatic termination.

7.0 Automatic Mainframe System Log-Off

All users must log off their mainframe network session (TPX) when leaving their terminals for more than 20 minutes.

All mainframe applications shall be configured to automatically terminate any user logged into an application whose terminal has been inactive for an additional 30 minutes after the automatic session termination. (See Section E.5) The mainframe applications shall be configured to terminate any mainframe connection that is running and require the user to re-authenticate his identity before resuming interaction with the system. An entry should be made in the audit trail for each automatic log off.

8.0 Secure Remote Access

Hardware security tokens, such as cryptographic smartcards, can be issued to employees and contractors who have a valid need to remotely access CBP systems and data. The process and procedures for obtaining secure remote access devices, user responsibilities, operating procedures, and other information pertaining to administration of the Secure VPN Communications Program are contained in Appendix M, User Agreements.

9.0 Warning Banner

IT systems internal to the DHS network shall display the approved Department Warning Banner.

IT systems accessible to the public shall provide the approved Department security and privacy statement at every entry point.

IT systems internal to the DHS and CBP networks shall display the approved Department Warning Banner. IT systems accessible to the public shall provide the approved Department security and privacy statement at every entry point. A log-on warning banner is required on all networked and stand-alone CBP IT systems. Section 2.2 of this handbook contains the approved Department Warning Banner that must be displayed on CBP systems.