



U.S. Customs and
Border Protection

Attachment W

User Agreements

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 User Agreements..... 3

2.0 User Knowledge of Security Standards 3

3.0 Dedicated Internet Access Agreement..... 3

4.0 Secure VPN Communications Access Agreement 7

 4.1 Background..... 7

 4.2 Procedure to Request Secure VPN Communications Access..... 7

This attachment details procedures to dedicate a standalone desktop for Internet access and to request remote secure Virtual Private Network (VPN) communications access.

1.0 User Agreements

1. User agreements contained in this appendix are used to either dedicate a standalone desktop for Internet access or to request remote secure VPN communications access. They also document authorized users' awareness of the required security standards for using a standalone desktop or secure VPN access.

2.0 User Knowledge of Security Standards

All users must be aware of the environment in which they perform day-to-day duties using CBP-owned information systems.

1. Be knowledgeable about the system security features and policies prescribed for each system you access.
2. Complete annual security awareness training as required by policy and regulations.
3. Report all security violations to the CSIRC immediately. Contact information for incident reporting is found in Section 5.6.
4. Obtain the proper authority or consent before releasing, disclosing, or altering information. For example, agents have disclosure authority and can routinely disclose Law Enforcement data, even if it is Office of Field Operations' data. Inspectors have no disclosure authority, even to disclose their own data.

3.0 Dedicated Internet Access Agreement

The Dedicated Internet Access Agreement is used to request permission to set aside a dedicated, standalone desktop computer system strictly for Internet access. It is a multi-part form that outlines user and system administrator responsibilities, in addition to certain security features that must be supported on the dedicated workstation. The agreement is available in softcopy from the CBP Intranet Web site at the following link:

(b)(7)(E)

It may also be obtained by sending an email to **(b)(7)(E)**. A sample is included as Figure M.3.


Any CBP official, with a job-related need to set aside a dedicated, standalone desktop computer system for Internet access, may submit the Dedicated Internet Access Agreement. The official should read the agreement and sign in the space provided. By signing, the official agrees to adhere to all conditions of the agreement, including closely monitoring the use of the dedicated workstation. All Internet access performed using the dedicated desktop system must be for authorized government business only, with no expectation of privacy. The dedicated desktop

system must not be used to process or store any sensitive information and must not be interconnected with any CBP system.

The Dedicated Internet Access Agreement must be completed, signed, and faxed (b)(6) (b)(7)(C) to the CISO in order to obtain a written one-year approval. The official establishing the dedicated, standalone desktop computer system will make appropriate arrangements with the Systems Administrator (SA) for system support. The SA will make every effort to ensure the workstation is used according to the agreement by accomplishing the following tasks:

1. Install and update anti-virus software on the computer. Install auditing software, if required.
2. Observe the use of the workstation to ensure that all use is for authorized government business only.
3. Remove violators from the workstation and report them to their supervisor.
4. Delete user accounts when the user no longer needs access due to transfer or any other reason.
5. Annually revalidate all established accounts and delete any inactive accounts.
6. Supervisors/managers will notify the SA when subordinate personnel no longer have a need to use the dedicated system.

Figure M.3: Dedicated Internet Access Agreement (Page 1)

	<p><i>Customs and Border Protection</i> <i>Dedicated Internet Access Agreement</i></p>			
<p>DEDICATED INTERNET ACCESS AGREEMENT FOR STANDALONE COMPUTER SYSTEMS</p>				
<p>1. Use of Dedicated Computer Systems for Internet Access. This agreement sets aside a CBP-owned dedicated computer system that shall be used for Internet access.</p>				
<p><i>An employee has a duty to protect and conserve government property, including computers and electronic data, and shall not use such property or allow its use for other than authorized purposes. (5 CFR Section 2635.704)</i></p>				
<p><i>Unless authorized in accordance with law or regulations to use such time for other purposes, an employee shall use official time in an honest effort to perform official duties. (5 CFR Section 2635.705(a))</i></p>				
<p>2. Use Internet Access Properly. The use of the system set aside in this agreement could reflect upon CBP if misused. All users shall avoid any action that might adversely affect the confidence of the public in the integrity of Customs and Border Protection, whether they are an employee or a contractor.</p>				
<p><i>Public service is a public trust. To ensure that every citizen can have complete confidence in the integrity of the federal government, each employee shall respect and adhere to the principles of ethical conduct set forth in the section, as well as the implementing standards contained in this part and in supplemental agency regulations. ... (14) Employees shall endeavor to avoid any actions creating the appearance that they are violating the law or the ethical standards set forth in this part. (5 CFR, Section 2635.101(a))</i></p>				
<p>3. System Administrator. The system being set aside for Internet access shall have a System Administrator responsible for ensuring its use in accordance with this agreement and applicable sections of <i>CBP Information Systems Policies and Procedures Handbook CIS HB 1400-05C</i>.</p>				
<p>4. Copyright Issues. The system being set aside for Internet access shall not be used to download copies of software or code unless an approved procurement process is used.</p>				
<p>5. CBP-Owned Data Issues. The system being set aside for Internet access shall not be used to process, store, retain or transmit any official CBP data or information of any nature.</p>				
<p>6. Configuration and Inspections. The system being set aside for Internet access shall only contain approved software and hardware installed by authorized CBP technicians. The system must not be connected to any other devices or LANs, physically or electronically, during the length of this agreement. For example, LAN-based printers may not be accessed by the system being set aside for Internet access. The System Administrator will periodically inspect the system to validate the proper hardware/software configuration.</p>				
<table border="1"> <tr> <td>06/01/2006 (Date Printed)</td> <td>Version 2.1, 06/01/2006</td> <td>Page 1</td> </tr> </table>		06/01/2006 (Date Printed)	Version 2.1, 06/01/2006	Page 1
06/01/2006 (Date Printed)	Version 2.1, 06/01/2006	Page 1		
<p>FOR OFFICIAL USE ONLY</p>				

• **Figure M.3: Dedicated Internet Access Agreement (Page 2)**

7. Virus Scanning Software. The system being set aside for Internet Access shall have a current copy of an approved anti-virus software installed and operating at all times.

8. Auditing Software. The System Administrator shall periodically inspect the cache memory, history files, cookies, etc., of the set aside system to determine if it has been used for inappropriate activities such as visiting pornographic sites, etc. As an option, the System Administrator is authorized to install audit software capable of monitoring and recording all information sent or received on the system.

9. System Location. The system being set aside for this agreement is located at the following address:

Computer PIMS Number _____

Street Address	Phone	Room Number
_____	_____	_____
City	State	Zip Code
_____	_____	_____

10. I, the undersigned CBP official, have read this Dedicated Internet Access Agreement and agree to comply with its provisions. I further understand that this agreement is valid for only one year and then this form must resubmitted with a new date.

Signature	Date
_____	_____

Printed Name	Telephone Number
_____	_____

CISO Signature	Date
_____	_____

CISO Printed Name	Telephone Number
_____	_____

06/11/2008 (Date Printed)	Version 3.0, 06/11/2008	Page 2
----------------------------------	--------------------------------	---------------

~~FOR OFFICIAL USE ONLY~~

4.0 Secure VPN Communications Access Agreement

4.1 Background

Many employees of the Department of Homeland Security components (e.g., CBP, ICE, FLETC) and participating government agencies require remote secure access to the National Data Center (NDC) in order to perform their official duties (e.g., telecommuting). The procedure below details how to request this type of remote access known as secure Virtual Private Network (VPN) communications access.

Currently, the project is fully funded nation-wide and is available to employees of all Department of Homeland Security components and participating government agencies who have a valid requirement for this type of access. However, employees must already have a notebook or laptop approved for use of secure VPN communications access. The notebook or laptop will be re-imaged with a patched Windows 2000 Operating System and up-to-date anti-virus software. The user should make sure that all stored work and important data is backed up before allowing the notebook or laptop to be re-imaged.

Secure VPN user accounts will be limited to a two (2)-year lifespan and are subject to renewal approval by the user's supervisor prior to expiration. Submission of another **Secure VPN Access Form** will be required to obtain access for an additional two-year period. This renewal process complies with audit requirements and best practices for government systems.

4.2 Procedure to Request Secure VPN Communications Access

(b)(7)(E)

(b)(7)(E)

The Secure VPN Communication Access Request Form must be completed by the requesting person with a valid VPN Access requirement. The agreement outlines certain Security requirements that must be observed by CBP remote access customers. The requesting individual reviews the specified requirements, from the Intranet Web page, complete the sections requesting your workstation information to assist the requestor to load the remote access software on his/her laptop or desktop. The requestors will need to provide the name of the Government Supervisor who will verify the need for access. Once the requestor fills out the page and submits the request, the Supervisor is notified via email of the request for access. The Remote Access team will ship the token or mobikey to the LAN Administrator, who will contact the requestor and subsequently gives the FOB to the User to safeguard. The requirement for remote access is automatically recertified using a web-based email notification process every 6 months.