Transportation Security Administration

Computer Access Agreement

1. PURPOSE

To obtain written agreement from all Transportation Security Administration (TSA) Information Technology (IT) systems users signifying understanding and acceptance of applicable policy and legal requirements concerning the operation of computer equipment and access to network resources within the TSA. This policy applies to all staff, interns, volunteers, and contractors assigned or detailed to TSA. This agreement is based on policy delineated in TSA Information Security Policy Handbook (MD 1400.3).

I hereby acknowledge my understanding of and agreement to comply with the following requirements:

1) Classified Processing. I will not process classified information on any TSA systems not specifically approved and marked for the appropriate level of classified processing. I will report to the designated official within the Office of the Chief Information Security Officer any inadvertent or unapproved classified processing on non-classified systems. I will not process classified information or store classified information on non-government issued devices or media.

2) Credential Protection. I will protect my passwords and any authentication tokens from disclosure and loss at all times. I will employ a password with a minimum of eight characters in length that will contain at least one uppercase alphanumeric, one lowercase alphanumeric, one numeric, and one special character. I will change my default passwords immediately when assigned. I will never reveal my passwords to other individuals. I will not construct my password from obvious personal data (i.e., social security number, telephone numbers, relative's names, pet's name, etc.).

3) User Accounts. I will not allow others to use my account and I will not access other users' accounts. I will not attempt to access accounts or data stores that are not expressly authorized to me without written authorization from a supervisory level government employee. I understand that I am accountable for all actions taken under my username. When using the account for personal business, I will abide by the TSA Policy for Personal Use of IT assets.

4) Data Protection. I will protect all data storage devices (i.e., disks, CD's, thumb or jump drives, etc.) in accordance with the highest level of data sensitivity contained on those storage devices. For data to be physically delivered to any entity outside of TSA, the storage device will either be new or will have been cleansed (all data overwritten or zeroed) of all but the data being delivered.

5) Physical Security. I will not remove TSA computer systems or software (desktops, infrastructure, or others not generally accepted as personal productivity tools (laptops and PEDs), from government workspaces without the express permission from the designated official. When laptops and PEDs, including PDAs, are in my possession outside government spaces, I understand I am personally responsible for providing physical security and keeping items under my exclusive control.

6) E-mail. I understand the government e-mail system is provided for the conduct of official TSA business. I will limit my non-official use of the e-mail system to prevent interference with my official duties or cause degradation of network services. E-mail systems are the property of the Federal government, and the Federal government owns the data stored on these systems including all messages, even those messages deemed personal by their authors. The fact information is produced or preserved electronically does not confer on it any status that is different from the same information in hard copy. I will not send e-mail that is malicious, deceptive, hostile, threatening, abusive, vulgar, defamatory, profane, or racially, sexually, or ethnically objectionable.

7) Internet Use. I understand access to public networks (i.e., the Internet) is for official TSA business. I will limit my non-official access to the Internet to prevent interference with my official duties or cause degradation of network services. I understand usage of the system will be in keeping with the Federal code of conduct. .

8) Unauthorized software. I understand it is forbidden to download any software from the Internet or non-TSA media. This includes instant messaging, file-sharing (i.e., Kazaa or AIM), or any freeware software tools. I will not load any software that has not received prior written authorization.

9) Consent to Monitor/Privacy. I understand the use of government furnished equipment constitutes my consent to monitoring and audit of this use at all times. I understand there is no expectation of privacy when using or storing data on government systems.

10) Protection of Displayed Data. I will logoff my computer when leaving my work area unattended for extended periods. I will use a screen saver that requires the reentry of my password when my system is idle for short periods of time. The exact length of time will be a local policy, depending on my local security environment.

11) Copyright Protection. I will not duplicate copyrighted software or remove copyrighted software from government equipment without the expressed written permission of the system administrator or IT Security Office. I understand I will be personally liable for any software copyright violations committed on government systems under my control.

12) Termination of Employment. Upon termination of my employment, I will ensure all equipment assigned to me is returned to the government. In addition, I will ensure all data is archived in an appropriate manner.

Signatures/Identification Data			
User Signature:	_____	**Date:**	_____
User Printed Name:	_____		
ID# (Last 4 of SSN):	_____		
Contractor/Contract/Company:	_____		
Or Government/Dept.:	_____		
Routing Symbol/Airport Code:	_____		
E-Mail Address:	_____		

1. DOCUMENT CHANGE HISTORY

Effective	Version	Explain the Change Action	By
2005.02.11	1.00	Initial release	G Chitwood
2005.06.30	2.00	Update ownership office and make consistent with forms management directive	G Chitwood

2. DOCUMENT CONTROL INFORMATION

Document ID	Document Owner	Change Approval Authority	Stored	Review	Disposition
TSA Form 1402	G. Chitwood	TSA ISSM	OIMP MD	Annually	

Note: Please Return To Supervisor – Supervisor Must Maintain Originals For IG And CISO Annual Audit

Privacy Act Statement

AUTHORITY: 5 U.S.C. § 301. **PRINCIPAL PURPOSE(S):** This information will be used to ensure that individuals have completed and understood information systems security awareness training. **ROUTINE USE(S):** This information may be shared with another training facility for training purposes, or for routine uses identified in OPM system of records, OPM/GOVT-1 General Personnel Records. **DISCLOSURE:** Voluntary; failure to furnish the requested information may result in a loss of computer access privileges.