



U.S. Department of Transportation
Office of the Secretary of Transportation

Cyber Security Assessment and Management Rules of Behavior

The Cyber Security Assessment and Management (CSAM) Rules of Behavior (ROB) is system-specific and addresses the terms for access to and use of the CSAM application. This ROB complements the general the ROB provided within the Department of Transportation (DOT) Cybersecurity Compendium, Appendix E: DOT Rules of Behavior. A supplement to DOT Order 1351.37 Departmental Cybersecurity Policy.

All CSAM Users must read and acknowledge the CSAM Rules of Behavior prior to being granted access and renew this acknowledgement annually. This is an Information System Security (ISS) requirement to help ensure CSAM Users are aware of the security considerations associated with utilization of the application and the data it maintains. This ROB includes a Digital Signature. We are currently accepting e-mail acknowledgements as electronic authorization. Please complete the ROB electronically and return to the CSAM Account Manager via e-mail to Keith.Guest@faa.gov to acknowledgment this ROB.

I will comply with Department of Transportation (DOT) policies, regulations and guidelines regarding the protection, handling, processing, transmission, distribution, and destruction of sensitive unclassified information designated "Sensitive Security Information (SSI)". SSI is a designation unique to the DOT and DOT's operating administrations and to the Department of Homeland Security (DHS). It applies to information we obtain or develop while conducting security activities, including research and development activities. Unauthorized disclosure of SSI would:

- (1) Constitute an unwarranted invasion of privacy (including, but not limited to, information contained in any personnel, medical, or similar file);
- (2) Reveal trade secrets or privileged or confidential information obtained from any person; or
- (3) Be detrimental to transportation safety or security.

[Privacy Act 1974 as referenced by DOT H1350.2.1](#)

I will protect sensitive unclassified information from unauthorized access, disclosure, modification, misuse, damage, or theft.

[Privacy Act 1974 as referenced by DOT H1350.2.1](#)

I will not copy or remove copies of Software licensed to DOT without proper authorization nor will I import or use unauthorized software, firmware, or hardware in the work environment.

[NIST 800-14 Sec 3.9](#)

I will protect all passwords issued to me and will not disclose them to anyone. I understand that password sharing or the use of another user's ID and password is prohibited. I will change my passwords when required by the system and whenever I suspect that they may have been compromised.

[DOT H1350.2 Sec 75 Part 3&4](#)

I will not embed passwords in log-on scripts.

[DOT H1350.2 Sec 75 part 3&4 or NIST 800-14 Sec 3.11.2](#)

I will report all security incidents, including password compromises, violations of software licensing agreements, and computer viruses, to the Security Official and/or my government project manager.

[DOT H1350.2 Sec 75 part 6 also NIST 800-14 Section 2.4](#)

Sensitive Security Information



U.S. Department of Transportation
Office of the Secretary of Transportation

Cyber Security Assessment and Management Rules of Behavior

I will immediately notify the Security Official for my area when I no longer require access to the network because of transfer, completion of project, etc., and of any changes in my work location or phone number.
[NIST 800-14 Section 3.5.2](#)

I will use the LAN for processing, transmission, and storage of official U.S. Government related or authorized work only.
[DOT 1350.272](#)

I will not knowingly introduce any malicious code into the network nor will I attempt to bypass or circumvent network security features or mechanisms.
[Computer Fraud and Abuse Act of 1986 \(as referenced by DOT H1350.2.1\) and NIST 800-14 Sec 3.7.1](#)

I will not relocate DOT network equipment or software without proper authorization.
[DOT H1350.2 Sec75 Part7](#)

I will use only DOT-configured equipment only in connecting to the CSAM application.
[NIST 800-53: Control AC-20](#)

Upon final checkout or departure from DOT, I will not have in my possession or in my home any sensitive-unclassified information in any form, nor any government-owned equipment, software, storage media (e.g. diskettes), user manuals, or system documentation.
[NIST 800-14 Section 3.5.2](#)

I understand that failure to comply with any or all of the above security requirements could result in the loss of my system privileges and or civil or criminal penalties
[DOT H1350.2 Sec 7C Part 6](#)

Sensitive Security Information



Cyber Security Assessment and Management Rules of Behavior

By signing this agreement, I understand and consent to the following when I access DOT's CSAM information system:

- I acknowledge that I have received a copy of these Rules of Behavior;
- I understand, accept and agree to comply with all terms and conditions of these Rules of Behavior;
- I am accessing a U.S. Government information system that is provided for U.S. Government authorized use only;
- The Government routinely monitors communications occurring on this information system. I have no expectation of privacy regarding any communications or data transiting the Government network or stored on its computer systems or storage media; and
- Any communications or data transiting or stored on DOT information systems or storage media may be disclosed or used for any lawful government purpose.

I understand and consent to these Rules of Behavior.

Name of User (printed):	
User's E-mail Address:	
DOT Operating Administration or Secretarial Office:	
Other Organization (Federal Agency or Contractor Company Affiliation):	
Location or Address:	
Supervisor's Name:	
User's Signature:	
Date:	

Sensitive Security Information