

U.S. Department of Transportation OST Information System User Responsibilities

A. General

1. OST information systems should be used primarily for official, mission-related DOT business. Limited incidental personal use that complies with the standards of ethical conduct is acceptable.
2. OST information systems cannot be used for commercial purposes, for financial gain, or in support of “for profit” non-government activities.
3. OST information systems are the property of the Federal government. DOT owns the data stored on these systems, including all e-mail messages and information, even those deemed personal.
4. Sensitive information will not be transmitted at a level higher than what the system is approved for.
5. Information that was obtained via the DOT systems will not be divulged outside of government channels without the express permission of the data owner.
6. Any activity that would discredit DOT, including seeking, transmitting, collecting, or storing defamatory, discriminatory, obscene, harassing, or intimidating messages or material is not permitted.
7. Any activity that violates Federal laws for information protection (e.g., hacking, spamming, etc.) is not permitted.
8. Virus protection tools must be installed and kept current on any and all machines from which the network is accessed.
9. Any security problems, password compromises, or anomalies in system performance must be reported immediately to security personnel.

B. Passwords

1. Passwords should be a minimum of eight characters, and be a combination of letters, numbers and special characters (such as *#\$%). Dictionary words should not be used.
2. Passwords will be changed at least every 90 days and should never be repeated. Compromised passwords will be changed immediately.
3. Passwords must be unique to each user and must never be shared by that user with other users. For example, colleagues sharing office space must never share each other’s password to gain system access.
4. Users who require multiple passwords should never be allowed to use the same password for multiple applications.
5. Passwords must never be stored in an unsecured location. Preferably, passwords should be memorized. If this is not possible, passwords should be kept in an approved storage device, such as a Government Services Administration Security Container. If they are stored on a computer, this computer should not be connected to a network or the Internet. The file should be encrypted.

C. Encryption

1. Extremely sensitive data should be encrypted prior to transmission.
2. The sensitivity of the information needing protection, among other considerations, determines the sophistication of the encryption technology. In most circumstances, only the most sensitive or compartmentalized information should be encrypted.
3. Files that contain passwords, proprietary, personnel, or business information, and financial data typically require encryption before transmission, and should be encrypted while stored on the computer's hard disk drive.
4. Sensitive information that travels over wireless networks and devices should be encrypted.

D. Internet Usage

1. Utilizing unauthorized peer-to-peer networking or peer-to-peer file sharing is prohibited.
2. Installing software that has not been authorized by the system administrator is prohibited.

E. E-mail

1. Except for limited personal use, non-work-related e-mail is prohibited.

F. Working from Home/Remote Dial-up Access

1. Remote dial-in access to OST information systems (e.g., OST internal systems) must be pre-approved system administrator.
2. Users must be certain to log-off and secure all connections/ports upon completion.
3. Users who work from home must ensure a safe and secure working environment that prevents unauthorized access to official information and the network..
4. Web browsers must be configured to limit vulnerability to an intrusion and increase security.
5. Home users connected to the Internet via a broadband connection (e.g. DSL or a cable-modem) must install a hardware or software firewall (e.g., Zone Alarm (<http://www.zonelabs.com>))
6. Users agree to protect the privacy and security of all DOT data and equipment in the same way that is required when working at the office.
7. Operating system configurations should be selected to increase security.

G. Additional Rules of Behavior for Users

1. Using system resources to copy, distribute, utilize, or install unauthorized copyrighted material is prohibited.

2. Users who no longer require IT system access (as a result of job change, job transfer, or reassignment of job responsibilities) must notify the System Administrator.
3. When not in use, workstations must be secured. Users must also log-off.
4. Attaching devices (e.g., laptops, printers, etc.) that have not been authorized by the system administrator is prohibited.
5. Movable media (such as diskettes, CD-ROMs, and Zip disks) that contain sensitive and/or official information must be secured when not in use.
6. Altering code, introducing malicious content, denying service, port mapping, engaging a network sniffer, or tampering with another person's account is prohibited.
7. If a user is locked out of the system, the user should not attempt to log-on as someone else. Rather, the user should contact the System Administrator.

Acknowledgment

My signature below indicates that I have read, understood, and will comply with these requirements. I also understand that failure to comply with the requirements may result in loss of account privileges and/or disciplinary action.

Name (please print)_____

Signature_____

Organization_____

Date_____