DOT General Rules of Behavior for IT Users

March 21, 2017

Version 4.0

General Rules of Behavior for Users of U.S. Department of Transportation (DOT) Systems and Information Technology (IT) Resources that Access, Store, Receive, or Transmit Information

1.0 Purpose

This policy sets forth the U.S. Department of Transportation's (DOT) General Rules of Behavior for IT users. The purpose of this policy is to define the responsibilities and the expected behavior of all individuals with access to DOT information and information systems. A primary mission of the DOT Office of the Chief Information Officer (OCIO) is to provide and support end-user computing devices, systems, applications, and network communication resources.

These resources are for the official use by DOT employees, contractors, and authorized third parties to meet the daily operational and mission requirements of the agency. IT users should have no expectations of personal privacy protection when using DOT owned IT resources. If an individual is found to be in violation of the Rules of Behavior, DOT reserves the right to take disciplinary action, including the restriction and possible loss of network privileges. A serious violation could, however, result in legal or disciplinary action, up to and including termination of employment and prosecution. DOT IT users are expected to be familiar with and comply with this policy, and are also required to exercise due diligence while using DOT IT resources.

2.0 Application

This policy applies to all users of IT owned or managed by DOT. Individuals covered by the policy include (but are not limited to) DOT employees, contractors, consultants, and third parties accessing DOT computing resources and IT systems. This policy shall apply to employees and contractors at their primary workplace or an alternate worksite. Computing resources include, but are not limited to, all DOT owned, licensed or managed hardware and software, and use of the DOT network via a physical or wireless connection, irrespective of the ownership of the computer or device connected to the network.

3.1 Roles and Responsibilities

3.2 Employees

DOT employees are required to read this document, understand the expectations, and assume personal responsibility for adhering to the provisions of the Rules of Behavior agreement. Each employee and end-user will be required to formally acknowledge through signature the receipt of this policy. DOT employees are hereby advised that that misuse or abuse of IT resources may lead to department or agency investigation and initiation of legal or disciplinary actions.

3.3 Contractors, Vendors, and other Third Parties

Agents, contract staff, vendors, and other third parties are required to acknowledge an awareness of this policy through signature of the applicable Rules of Behavior agreement, adhere to the

requirements contained therein, however realizing that the consequences of violation will be appropriate to their status.

Departmental personnel involved in procurement or contract management matters must communicate this policy to vendors who will use DOT IT resources and/or include a provision in all new contracts and contract modifications that requires the vendor to ensure all contract staff acknowledge the ROB, in writing or electronically, and maintain the acknowledgement.

3.4 Managers and Supervisors

Managers and supervisors make up the first line of accountability for staff compliance with this policy and shall require that all personnel read, acknowledge, and comply with the DOT Rules of Behavior and the federal and DOT policies referenced in this directive.

4.0 Procedures

IT users are required to review the DOT Rules of Behavior and sign an acknowledgement form annually. As updates are made, a new acknowledgement form must be signed. The Office of the DOT Chief Information Officer (DOT OCIO) makes this policy available to employees through the DOT online learning management systems (LMS). Contractors can also access the policy while completing the annual DOT Security Awareness Training (SAT). Users are encouraged to submit the acknowledgement form online through their respective training systems; however, the signed acknowledgment can be submitted manually to the designated Operating Administration (OA) point of contact and the Privacy Officer of the employing DOT OA. The failure to submit a signed acknowledgement form can result in information system access denial, revocation of assigned information system access, and/or other administrative sanctions.

DOT Components are responsible for developing any system-specific guidelines necessary to complement the *General Rules of Behavior*. The guidelines must be signed by the user before access to the system and/or network is approved.

5.0 Effective Date

This policy is effective immediately.

6.1 References

a. Appendix III, Office of Management and Budget (OMB) Circular A-130 – Security of Federal Automated Information Resources;

b. Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C.§3541

c. DOT Order 1351.37 Departmental Cybersecurity Policy

d. DOT Cybersecurity Compendium

e. DOT Order 1351.33 Departmental Web-Based Interactive Technologies Policy (Social Media and Web 2.0), Appendix A (Employee Conduct Policy)

Enclosure(s)

Enclosure 1 – DOT General User Agreement for IT Rules of Behavior

APPROVED: _____

Andrew R. Orndorff

Associate CIO / Chief Information Security Officer

U.S. Department of Transportation

ENCLOSURE 1

U.S. Department of Transportation General

User Agreement for IT Rules of Behavior

DOT technological and information resources are for the official use by staff to meet the daily operational and mission requirements of the agency. This policy describes the responsibilities and expected behavior of all individuals that have access to DOT information systems. As an authorized user, you are responsible for exercising good judgment regarding the appropriate use of DOT resources in accordance with applicable federal and DOT policies, standards, and guidelines. Users should have no expectations of personal privacy protection when using DOT owned technologies and resources. By accessing DOT IT resources, you agree to adhere to the Rules of Behavior set forth in this policy. The DOT Rules of Behavior apply to users at their primary workplace, while teleworking or at a satellite site, at any alternative workplaces, and while traveling.

1. **System Accounts, Passwords, and other Access Control Measures**
   a. I understand that DOT systems are intended for official-use only, and that I am authorized to use only those systems for which access is required to execute my official duties. I will not attempt to access systems or information I am not authorized to access.
   b. I understand that I have no expectation of privacy while using any DOT equipment or while using DOT networks, internet or e-mail services.
   c. I acknowledge that I am responsible for the security of data, accounts, and systems under my control, or to which I've been granted access. I will safeguard the information processed, stored, and transmitted on DOT information systems from unauthorized or inadvertent disclosure, modification, destruction, and misuse.
   d. I will keep my passwords secure and not share account or password information with anyone. I agree to maintain system-level and user-level passwords in accordance with the DOT password policy. I understand that providing system access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.
2. **Computing Assets**
   a. I understand that DOT information systems consist of: 1) my desktop or laptop; 2) DOT computer networks; 3) DOT-owned computers and devices connected to the DOT network; and 4) DOT-owned portable electronic and mobile devices and storage media attached to DOT networks or its computers.
   b. I will not attempt to bypass access control measures.
   c. I will not use personally-owned equipment to access DOT information systems and networks or process DOT information unless I am given expressed written approval from the system Authorizing Official, Component ISSM, or Component CIO. If I am granted permission to use personally-owned equipment for access to DOT information systems or networks:
      i. I agree to allow authorized DOT personnel to examine the personal IT device(s) that I have been granted permission to use, whether remotely or in any setting, so long as the personal devices are used to access or process DOT information.

ii. I agree to use DOT-approved encryption, virus protection software, anti- spyware, and firewall/intrusion detection software and ensure the software is configured to meet DOT configuration requirements prior to connection to DOT networks. Verification of configuration is performed by the Component CIO office.

3. **Network Use**

   a. I understand that Internet activities that may compromise the safety and availability of DOT information and information systems, or cause degradation of network services, are prohibited unless otherwise permitted for official duties. Examples of such activities include streaming of audio or video, peer-to-peer networking, and attempted unauthorized access to DOT or other organizations' information systems.

   b. I agree to comply with all software copyrights and licenses.

   c. I will not install unauthorized software (including software available for downloading from the Internet, software available on DOT networks, and personally owned software) on DOT equipment (e.g., DOT workstations, laptop computers, PEDs).

   d. I will not host, set up, administer, or operate any type of internet server on any DOT network or attempt to connect any equipment to a DOT network without the express authorization of my Component CIO. If such authorization is granted, I will ensure that all activity is performed in accordance with DOT security guidelines and policies.

   e. I will not use peer-to-peer (P2P) file sharing to connect remotely to other systems for the purpose of sharing files. I understand that P2P file sharing can be a means of spreading viruses over DOT networks and may put sensitive government information at risk. I also understand that DOT Order 1351.37 Department Cybersecurity Policy through its Cybersecurity Compendium prohibits the use of P2P software on any DOT-owned, controlled or operated equipment.

4. **E-mail, Social Media, and Other Electronic Communications**

   a. I understand that I must use internet web-based technologies such as social media/networking, blogging and messaging, as outlined in DOT Order 1351.33, Appendix A: Employee Conduct Policy.

   b. I understand that DOT-provided internet and e-mail is for official use, with incidental personal use allowed.

   c. I will not forward or copy DOT e-mail messages to my personal email account or addresses outside the DOT network.

   d. I understand that the use and access to internet webmail such as Yahoo, Google and MSN or access to other personal email accounts from DOT information systems is permitted to the extent that it constitutes no more than incidental personal use.

   e. I will not provide personal or official DOT information solicited by e-mail. I will be on alert if I receive e-mail from any source requesting personal or organizational information. If I receive an e-mail message from any source requesting personal information or asking to verify accounts or security settings, I will forward the message to the appropriate DOT Help Desk and delete the message from my system.

5. **Consent to Monitoring Provision**

   a. I understand that the communications and data stored on DOT information systems are not private, are subject to routine monitoring, interception, and search, and may be

disclosed or used for any U.S. Government-authorized purpose.

b. I understand that the viewing of pornographic or other offensive or graphic content is strictly prohibited on DOT furnished equipment and networks.

6. **Data Protection and Privacy**

a. I understand that I must complete mandatory periodic (at least annual) security and privacy awareness training within designated timeframes and must complete any additional system-specific required training for the particular systems to which I require access.

b. I will not leave smart cards unattended, on or with DOT workstations, laptop computers, or Personal Electronic Devices (PEDs).

c. I understand that I am permitted to access DOT information systems and networks from DOT-provided office equipment (e.g., workstations, laptops, PEDs).

d. I will use DOT-provided encryption to encrypt any e-mail, including attachments to the e- mail, which contains DOT sensitive information or PII before sending the email.

e. I will not send any e-mail that contains DOT sensitive information in an unencrypted form. DOT sensitive information includes but is not limited to Personally Identifiable Information (PII).

f. I will not store or transport any DOT sensitive information on personally owned devices such as my home computer, portable storage media or device unless it is encrypted using DOT-approved encryption.

g. I will use the PIV card issued to me for access to all systems where my PIV card is recognized.

h. I will protect sensitive information including PII from disclosure to unauthorized persons or groups.

i. I will ensure the proper handling of government records according to the orders, policies, and regulations which govern them.

j. I will not release such information unless specifically authorized to do so, or as required, on a “need-to-know” basis, in the proper discharge of official duties.

k. I will not divulge any official information obtained through or in connection with my government employment to any unauthorized person or organization.

l. I will not use, or permit others to use, any official information that is not available to the general public for private purposes.

m. I will not remove official documents or records from files for personal or inappropriate reasons. Falsification, concealment, mutilation, or unauthorized removal of official documents or records, either hard copy or electronic, is prohibited.

n. I will not disclose any PII or information contained in Privacy Act records, unless explicitly authorized and in compliance with DOT obligations under the Freedom of Information Act, the Privacy Act, or other federal law.

o. I will log off or lock my workstation or laptop computer, or I will use a password-protected screensaver, whenever I step away from my work area, even for a short time; I will log off or shut my workstation or laptop computer down when I leave for the day.

p. I will properly dispose of DOT sensitive information, either in hardcopy, softcopy or electronic media formats (CD, DVD, USB sticks) in accordance with DOT policy and procedures.

q. I will not access, process, or store classified information on DOT office equipment that has not been authorized for such access, processing or storage.

7. **Teleworking**

a. I will comply with DOT Telework Policy DOT Order 1501.1A.

b. I understand that I am responsible for safeguarding all DOT information, protecting DOT-furnished equipment, and performing assigned duties while teleworking.

c. I will utilize DOT-furnished computer equipment, software, and communications, with appropriate security measures for any telework arrangement that involves DOT data, unless prior written authorization is obtained from my Component CIO.

d. At my alternate workplace, I will follow security practices that are the same as or equivalent to those required of me at my primary workplace.

e. I will protect sensitive data at my alternate workplace. DOT Telework Policy specifies guidelines for "Safekeeping of Government Materials/Documents/Equipment." DOT Telework Policy also requires that all Sensitive Personally Identifiable Information (SPII) only be used when computing media/storage is encrypted with DOT-approved encryption solutions.

8. **Foreign Travel**

a. All DOT and Federal data must be encrypted using a DOT-approved encryption solution.

b. I understand that the use of loaner equipment is required for international travel. I will take DOT equipment on international travel only if the equipment is necessary to perform my official job duties.

c. I will take DOT internal information on international travel only if the information is required to accomplish official duties. I will take only the minimum amount of information required to accomplish DOT duties during travel.

d. I will ensure that all DOT equipment and any devices containing DOT information remain in my possession or are appropriately safeguarded while outside the United States and territories.

e. I will use the DOT CISCO AnyConnect Virtual Private Network for all business communications. I understand that any communication must be made only through an approved DOT VPN.

f. I will disable all Wi-Fi devices when not in use and refrain from using Bluetooth connections for any reason.

g. I understand that connecting any personal external media or technology to loaner equipment is strictly prohibited.

h. I acknowledge that this policy also applies to visits and meetings to facilities that are owned by or under the control of non-U.S. entities, even when the facilities are within the United States and territories.

i. I will report any loss, damage, or tampering of DOT equipment or any devices containing

DOT information to the DOT SOC immediately or within one (1) hour of the incident occurring.

j. I understand that all work-related activities conducted abroad must comply with DOT policies on international travel and the DOT Mobile Computing Device User Agreement.

9. **Laptop Computers and Portable Electronic Devices (PEDs)**

a. I will only use DOT-issued devices (workstations, laptops or PEDs) to access DOT systems and process DOT information.

b. I will password-protect any BlackBerry device, iPhone, or other PED that I use to process DOT information. I will set the security timeout feature to 15 minutes so that the device automatically locks and requires a password to unlock. Assistance can be obtained through the appropriate DOT Help Desk.

c. I will keep the laptop or PED under my physical control at all times, or I will secure it in a suitable locked container under my control.

d. I will take all necessary precautions to protect any laptop/PED in my charge against loss, theft, damage, abuse, or unauthorized use by employing lockable cases and keyboards, locking cables, and when possible encrypted removable media.

e. I will keep antivirus and firewall software installed and up to date on any computer system/laptop in my charge.

f. I will use only DOT-authorized internet connections that conform to DOT security and communications standards.

g. I will not make any changes to the system configuration of any laptop/PED in my charge unless I am directed to do so by a DOT system administrator or ISSM.

h. I will not program any laptop/PED in my charge with sign-on sequences, passwords, or access phone numbers.

i. I agree that I will not have both a DOT network connection and any kind of non-DOT network connection (including a modem or phone line or wireless network card, etc.) physically connected to any computer at the same time unless the dual connection is explicitly authorized in writing by my Component CIO.

j. I understand and will comply with the requirement that sensitive information stored on any laptop computer, PED or mobile media such as USB drives and CD/DVDs used outside of DOT-protected facilities must be encrypted using DOT-approved methods.

k. I understand and will comply with the requirement that sensitive information transmitted from wireless devices must be encrypted using DOT approved encryption methods.

l. I understand that the use of Bluetooth and other wireless communications is restricted on DOT information systems and that I must obtain permission for its use from the Component CIO.

m. I will immediately report suspected or actual IT security incidents or privacy breaches to the DOT's Security Operations Center (SOC). DOT SOC Phone: 1-866-580-1852, Option 1 DOT SOC Email: 9-AWA-SOC@faa.gov.

I acknowledge receipt of the *DOT IT General Rules of Behavior*, understand my responsibilities, and will comply with these provisions when accessing DOT information technology resources.

Name:	
Date:	
Signature:	
Operating Administration:	

* If you sign this digitally using your PIV card, then you only need to fill the *Signature* box.