FAA Rules of Behavior

Version 1.0 – August 2016

A. The FAA:

(1) Requires the use of this Rules of Behavior throughout the FAA.

(2) Must ensure that individuals have the proper clearance, authorization, and need-to-know before providing access to any FAA device, system, network, or information.

(3) May intercept, record, review, and report to law enforcement or other Federal departments and agencies, as appropriate, any wire, oral, and electronic communications while those communications are being made on, are in transit on, and when they are stored on FAA’s Information Systems. This includes email, telephone conversations, and data stored electronically on any device.

(4) Will hold users responsible for the compromise of Government systems, networks, or information through negligence or a willful act.

B. These Rules of Behavior will help guide users in the proper handling of FAA systems, networks, and information.

1. User Responsibilities

A. You have no reasonable expectation of privacy regarding communications or data transiting or stored on FAA’s information systems, including communications or data allowed for limited personal use. At any time, and for any lawful Government purpose, the Government may monitor, intercept, and search any communication or data transiting or stored on FAA’s information systems. Any communications or data transiting or stored on FAA’s information systems may be disclosed or used for any lawful Government purpose. Unauthorized or improper use of FAA’s information systems may result in disciplinary action up to and including removal, as well as civil and criminal penalties.

B. All users of FAA systems, networks, services, or information:

(1) Must comply with all Federal laws and DOT and FAA policies as implemented.

(2) Must use FAA systems and information for lawful, official use, and authorized purposes only, with limited personal use permitted.
(3) Must take personal responsibility for the security and protection of equipment provided to them, the systems they access, and the information contained on those systems.

(4) Keep their FAA profile up-to-date with all pertinent information to include contact information, organizational information, phone numbers, and supervisor information. This information is essential in emergencies. Users must review and update their FAA profile information at least annually or whenever there is a change in the users’ information, such as a move, relocation, reorganization, or other significant event.

C. Since written guidance cannot cover every contingency, personnel must go beyond the stated rules and use due diligence and the highest ethical standards to guide their actions. The FAA Rules of Behavior are based on Federal laws, OMB, NIST, and other guidance, as well as DOT and FAA policies and best security practices.

2. Applicability

A. These Rules of Behavior apply to all FAA bargaining and non-bargaining employees, supervisors, managers, executives, political appointees, contractor personnel, interns, students, detailers, service providers, and all other personnel that use or access FAA information systems, networks, and information technology (IT) resources, such as workstations, laptops, computers and portable electronic devices (PED) to access, store, receive, or transmit FAA information.

B. These Rules of Behavior apply to users at their primary workplaces, any alternative workplaces (e.g., telecommuting from home or from a satellite location), and while on travel.

C. System and network administrators and others with elevated privilege accounts must adhere to the additional rules of behavior specified in Section 10 ROB for System Administrator and Privileged Account Users.

D. Political Appointees must comply with all FAA security policies, however different rules for lobbying and political activity apply to employees appointed by the President and confirmed by the Senate. Those employees should consult FAA Order 3750.7A, Ethical Conduct and Financial Disclosure (as amended), for the FAA Ethical Code of Conduct and Financial Disclosure Program located at http://www.faa.gov/documentLibrary/media/Order/3750.7A.pdf or see the Human Resource Policy Manual (HRPM) ER-4.1, Standards of Conduct located at https://employees.faa.gov/ehr/hrp/er/er-4-1/ for guidance.

E. Federal law mandates that all FAA information system users must acknowledge and sign the FAA Rules of Behavior at least annually. The FAA may deny users who do not acknowledge
and sign (digitally or in writing) the Rules of Behavior access to FAA systems, networks and information.

3. **System and Data Access Protections**

   A. All FAA systems, networks, printers, phones, devices, equipment, software, services, and supplies, are for official FAA business use only, with **limited personal use** permitted.

   B. To protect FAA systems and data:

      (1) I will:

         a. Only attempt to access those systems for which I require access to perform my official duties.

         b. Complete the mandatory annual Security and Privacy Awareness Training and all additional system-specific required training within the designated timeframes.

         c. Only use FAA-provided or FAA-approved devices to connect to FAA systems and networks. Contact the FAA MyIT Service Center at 1-844-FAA-MyIT (1-844-322-6948) or via email at helpdesk@FAA.gov, or visit the https://MyIT.faa.gov Web site for more information on how to obtain approval to use non-GFE.

         d. Log off or lock my system whenever I step away from my work area, even for a short time. I will log off or shut down my GFE when I leave for the day.

         e. Encrypt all FAA **Controlled Unclassified Information (CUI)** and **Personally Identifiable Information (PII)** both in storage and in transit.

            ((1)) I will only store CUI and PII on GFE, approved non-GFE, and FAA-approved storage media such as USB drives, external hard drives CDs, DVDs, etc.

            ((2)) I will only use FAA-provided encryption methods that are FIPS 140-2 compliant, unless an applicable exception has been granted by the FAA Chief Information Security Officer (CISO) and the Chief Privacy Officer (CPO).

         f. Report the loss or theft of my GFE (and any approved non-GFE that contains or may contain FAA CUI or PII data) to the FAA SOC at 9-AWA-SOC@FAA.GOV, or by phone at 1-866-580-1852, Option 1.
((1)) If the system contains PII, or may contain PII, you must report the loss to the FAA SOC within one hour of discovering it missing.

((2)) You must report the loss of all other GFE within 24 hours of discovering it missing.

g. Use due diligence to keep my GFE under my physical control at all times.

(2) I will NOT:

a. Use personally owned equipment (POE), contactor-owned equipment (COE), or other non-Government Furnished Equipment (non-GFE) to access FAA information systems and networks or process FAA information unless I am given express written approval from the FAA Chief Information Officer (CIO) or designee. This includes but is not limited to laptops, desktop computers, tablets, thumb drives and other USB devices, printers, cameras, microphones, smartphones, or any device that is not approved for use on FAA systems or network.

b. Connect my GFE or approved non-GFE to the FAA network and to another network at the same time.

((1)) Connecting GFE and approved non-GFE to another network at the same time you are connected to the FAA network creates a path that can permit malicious users to access FAA systems and networks with your credentials.

((2)) Connecting to the FAA VPN will block access to all networked local printers, computers, and other devices connected to the local network. Refer to Section 7, Teleworking for additional information on connection to home networks.

c. View pornographic, offensive, or graphic content.

d. Aside from the limited personal use of FAA’s information systems permitted under these ROB, I will not store personal audio, video, photos, or any other personal files on FAA equipment, networks, or systems.

e. Attempt to bypass FAA-installed security control measures.

f. Attempt to access systems or information that I am not authorized to access.

g. Send, copy, or forward any FAA information that I am not authorized to send.
h. Take any GFE with me while on personal foreign travel, unless approved by the FAA (See Section 8, Foreign Travel with GFE for further information on this process).

i. Allow unauthorized personnel (including my family members) to use or access GFE assigned to me.

j. Access, process, or store classified information on any system or equipment that is not authorized for such access, processing, or storage.

k. Copy or distribute intellectual property – including music, software, documentation, and other copyrighted materials – without permission or license from the copyright owner.

C. If I have questions, concerns, or need to report issues with my GFE, I will contact the FAA MyIT Service Center at 1-844-FAA-MyIT (1-844-322-6948) or via email at helpdesk@FAA.gov, or visit the https://MyIT.faa.gov Web site.

4. Passwords and Other Access Control Measures

A. I will protect passwords, PINs, and access numbers from disclosure and I will not share passwords with anyone, including System Administrators.

B. FAA policy prohibits users from storing passwords and/or PINs on any non-encrypted electronic file or in any unlocked storage container. Users may write down passwords and/or PINs and store them in an appropriate locked storage container. Users may store passwords and/or PINs in an electronic file that is encrypted with FAA-provided or approved encryption software that is FIPS 140-2 compliant.

C. I will not leave my PIV card unattended with my GFE.

5. Privacy

A. Appendices 19 through 26 of the Information Security and Privacy (IS&P) Policy, and OMB M-07-16, Safeguarding and Responding to the Breach of Personally Identifiable Information, state that you must agree to:

(1) Not exceed your authorized access to PII.

(2) Not disclose PII to unauthorized persons.

(3) Report any known or suspected loss of control or unauthorized disclosures of PII to the FAA SOC within one hour at 1-866-580-1852, Option 1, or by email at 9-AWA-SOC@faa.gov.
(4) Maintain security controls for PII, which you are responsible and aware.

(5) All FAA employees and contractors must comply with the FAA Human Resources Policy Manual (HRPM) ER-4.1, Standards of Conduct, Section 4, Safeguarding and Use of Information, Documents, and Records.

B. If you have questions about the protection of PII, direct them to the Information Security and Privacy Service (AIS) at privacy@faa.gov or 1-888-PRIVAC1 (1-888-774-8221).

6. Internet, Email, and Social Media Use

A. FAA-provided Internet and email is for official use, with limited personal use allowed.

B. The FAA does not permit activities on the FAA’s information systems that affect the confidentiality, integrity, or availability of FAA systems or information, or cause degradation of network services.

(1) I will:

   a. Follow all FAA and DOT policies on the use of FAA Internet access, email, and use of social media.

   b. Be attentive to scams, phishing emails, social engineering activities that seek to obtain personal and FAA information through false pretense and deception. Such activities seek to obtain access to personal information to steal the users’ identity, gain unauthorized access to FAA systems and information, disrupt the FAA’s mission, or harm the FAA’s reputation.

   c. Validate the requestors’ need-to-know before providing any personal or FAA information.

(2) I will NOT:

   a. Play non-business related audio or video on any FAA system or network.

   b. Auto-forward my FAA email to any non-FAA email addresses, including my personal email address.

   c. Use peer-to-peer (P2P) file sharing software.

   d. I will not make statements on my personal social media Web sites that may be misconstrued as being made in an official FAA capacity. Please see the FAA social media Web site located at https://my.faa.gov/tools_resources/social_media.html.
e. Post any FAA documents, data, pictures, graphics, charts, etc. on my personal social media Web sites that the FAA has not made officially available to the general public.

C. The use of and access to personal Internet Web mail from FAA information systems is permitted to the extent that it constitutes no more than limited personal use, does not inhibit my work, and is done on my personal time.

1. While I am using my personal email account from the FAA network, I will exercise caution when accessing my personal email, opening attachments, and clicking on links, so that I do not introduce malicious software into the FAA environment.

2. Under no circumstance will I use my personal email account to conduct FAA business, unless I am authorized in writing by the FAA CIO or designee.

7. **Teleworking (From Home or a Satellite Center)**

A. FAA employees designated and approved to telework must have a signed teleworking agreement in place before beginning to telework, and must comply with FAA policies and the terms specified in the telework agreement.

B. From my alternate workplace, I will:

1. Use only FAA-provide GFE and approved non-GFE to connect to the FAA network.

2. Follow security practices that are the same as or equivalent to those required at my primary workplace.

3. Connect to the FAA network using approved virtual private network (VPN) connections.

C. I will not:

1. Connect my GFE or my approved non-GFE to other networks while I am connected to the FAA network through means including wired Ethernet, wireless (Wi-Fi), USB, Bluetooth, cellular, or other technology.

2. Store CUI, PII, and other sensitive FAA information on non-GFE unless I have authorization from the FAA CISO and CPO.

D. I am permitted to connect my GFE to my personal home network to log on to the FAA network and I may connect my personal monitor, keyboard, mouse, and printer to my GFE. If my personal devices require the installation of driver, I will contact the FAA MyIT Service.
Center at 1-844-FAA-MyIT (1-844-322-6948) or via email at helpdesk@FAA.gov, or visit the https://MyIT.faa.gov Web site.

E. When using FAA approved non-GFE devices, I will:

(1) Protect the confidentiality of Government information when using remote access (e.g., Outlook Web Access (OWA), Electronic Learning Management System (eLMS), MyAccess, etc.).

(2) Maintain a reasonable security posture (e.g., updated antivirus, local firewall, updated Operating System (OS), and software patch levels).

(3) When downloading attachments or files, I will immediately remove any extraneous attachments, encrypt them locally, or transfer them to an approved encrypted USB drive.

F. When using public non-GFE (computers at public libraries, hotel business centers, training facilities, etc.) I will:

(1) Not download attachments or files on public non-GFE.

(2) Delete attachments, files, and browser sessions when finished on public non-GFE.

(3) Not print emails in public areas or from public non-GFE printers. Users may print with non-GFE private printers at home if directly connected to their GFE or approved non-GFE.

G. The FAA may terminate or suspend teleworking at any time for any reason.

H. My supervisor may revoke my telework privilege if I do not comply with my telework agreement.

I. For additional information on teleworking, refer to the FAA telework policy located at: https://employees.faa.gov/org/staffoffices/ahr/program_policies/policy_guidance/hr_policies/hrpm/wl/wl-12-3/media/hrpm_ch_wlb-12.3_faa_telework_program.pdf.

8. Foreign Travel with GFE

A. When required to travel outside of the continental United States (OCONUS) for official FAA business, prior to departure I will Contact the FAA MyIT Service Center the FAA MyIT Service Center at 1-844-FAA-MyIT (1-844-322-6948) or via email at helpdesk@FAA.gov, or visit the https://MyIT.faa.gov Web site to:

(1) Determine if current security policies require me to take travel loaner GFE.
(2) And/or establish a temporary travel email account to reduce the risk that unauthorized persons will gain access to FAA’s information systems or FAA information.

B. More information on foreign travel is located at https://my.faa.gov/content/dam/myfaa/org/linebusiness/avs/offices/air/div_dir/ane/travel/travel_electronics.pdf.

C. Upon return from foreign travel, I will not connect any device I carried with me to an FAA system or network until the device is scanned for malicious code and is approved for reconnection to the FAA.

9. Incident Reporting

A. I will immediately report suspected or actual IT security incidents or privacy breaches to the FAA’s Security Operations Center (SOC) at 1-866-580-1852, Option 1, or by email at 9-AWA-SOC@faa.gov.

B. I will follow the instructions provided by the FAA SOC or the FAA service center representative to support investigation of the incident.

10. ROB for System Administrator and Privileged Account Users

A. All FAA system and network administrators, account administrators, and other privileged account users must:

   (1) Protect all privileged user account passwords, passcodes, Personal Identity Verification (PIV), personal identification numbers (PINs), etc. from unauthorized use, disclosure, or access.

   (2) Comply with all system and network administrator responsibilities specified in FAA policy.

   (3) Use privileged accounts for official and authorized administrative actions only.

   (4) Complete all specialized role-based training.

B. I will not:

   (1) Share my privileged account access, passwords, PINs with anyone.

   (2) Install or remove any system hardware or software, or modify any system setting, that I am not authorized to change.
(3) Provide anyone (including myself) with privileges or access greater than is necessary to accomplish assigned roles and responsibilities.

(4) Delete or modify audit logs, or prevent the auditing of privileged actions.

(5) Use a privileged account to perform activities that can be achieved with lower level access privileges, such as reading email, writing documents, and accessing Web sites (unless the activity is to perform administrative tasks on the Web site).

11. Acknowledgment Statement

A. I understand and acknowledge that the terms and conditions in this Rules of Behavior apply to my access to, and use of, FAA-owned or FAA-controlled systems, networks, and information including Personally Identifiable Information (PII) and other FAA Controlled Unclassified Information (CUI).

B. I understand that failure to comply with these Rules of Behavior could result in oral or written warning, suspension and/or removal of system access, reassignment to other duties, criminal or civil prosecution, suspension from duty, termination of employment, removal from a contract for contractor personnel, or any combination of the foregoing. Consequences of failure to comply will be commensurate with the individual’s level of responsibility and the nature of the violation. See the FAA Human Resources Policy Manual (HRPM) ER-4.1, Standards of Conduct, Section 4, for additional details.

C. I understand that willful unauthorized disclosure of FAA CUI, including PII, may result in legal liability for the offender. Individuals who demonstrate egregious disregard or a pattern of failing to comply with the listed requirements will have their authority to access information systems promptly revoked.

D. I may be required to sign additional specific or unique rules of behavior in order to access or use specific FAA systems.

E. By signing this agreement (electronically or in writing), I acknowledge that I understand and consent to these Rules of Behavior when I access FAA systems, network, or information.

F. If you do not accept the rules of behavior, you must not access any FAA device, system, network, or information.

☐ I acknowledge that I have read, I understand, and I agree to comply with all terms and conditions of these Rules of Behavior.
12. Definitions

A. **Contactor-owned equipment (COE)** is any equipment, device, or software that is purchased, owned, and maintained by an entity under contract with the FAA where the FAA does not have any ownership rights to such equipment, device, or software. The FAA prohibits the connection of COE to any FAA System or network without the express written consent of the FAA CIO, CISO or their designee. All COE must follow FAA procedures for approval and connection to FAA systems and networks.

B. **Controlled Unclassified Information (CUI)** is any information or data that the loss of, misuse of, unauthorized access to, or unauthorized modification of which, could adversely affect the national interest, the conduct of Federal programs, or the privacy of individuals. There are several synonyms to CUI including but not limited to SUI (Sensitive Unclassified Information). See FAA Order 1600.75, Protecting Sensitive Unclassified Information (SUI) (as amended) for further information.

C. **FAA Information** consists of all data, documents, and records, that FAA and contracted entities create, enter, collect, generate, and synthesize, in support of or during the conduct of the FAA business and mission. It includes but is not limited to printed and electronic documents, streamed data, spreadsheets, databases, files, decisions, system data (e.g., IP addresses, routing information, system names, etc.), operational air traffic control information, financial transactions, security information, vulnerabilities, etc.

D. **FAA’s Information Systems** consist of 1) my Government Furnished Equipment (GFE) desktop computer or laptop, 2) FAA computer networks and systems, 3) all computers connected to FAA computer networks and systems, 4) all other GFE (e.g., BlackBerry, iPhone, iPad, Portable Electronic Device (PED)), and 5) all devices and storage media (e.g.,
thumb drives, flash drives) attached to FAA networks or systems or to a computer on such a
network or system.

E. **FIPS 140-2** is a U.S. Government computer cryptographic security standard specified by the
National Institute of Standards and Technology (NIST). The Federal Information Processing
Standards (FIPS) 140-2 standard specifies the security requirements for cryptographic
modules and is used to accredit cryptographic modules for use by U.S. Government systems
to protect Sensitive Unclassified Information. FIPS 140-2 encryption protects the
confidentiality and integrity of the information that is stored on a computer system or is
transmitted across a network or other communications mechanism.

F. **Government Furnished Equipment (GFE)** is any device, equipment, supplies, media, etc.,
that the FAA provides to fulfill the FAA Mission and conduct official business and to
facilitate employee and contractor support of the FAA’s mission and official business.

G. **Limited Personal Use** means activities, events, or communications that the user conducts on
FAA information systems or networks for purposes other than accomplishing official or
otherwise authorized activities, does not adversely affect the employee's job performance, is
of negligible cost, and is limited to those situations where the Government is already
providing equipment or services, such as Internet and email. Limited personal use activity
must be of short duration and infrequent occurrence. All activities performed on the FAA
systems and networks are subject to interception and monitoring, including personal account
information and passwords. The FAA does not permit activities on the FAA’s information
systems that affect the confidentiality, integrity, or availability of FAA systems or
information, or causes degradation of network services.

H. **Non-Government Furnished Equipment (non-GFE)** is any device, equipment, supplies,
media, desktop, laptop, system, smartphone, tablet, or other device not owned or furnished
by the FAA. It includes but is not limited to equipment that you purchased or was gifted to
you, contractor-owned equipment, vendor-owned equipment, and other equipment not
purchased directly or indirectly by FAA and that is legally owned and controlled by a person,
contractor, vendor, department, or agency other than the FAA.

I. **Peer-to peer (P2P)** file sharing technology is a popular way for two or more persons to
initiate a communication session and share computing capabilities without a central network.
The P2P file sharing applications are readily available on the Internet and used to exchange
and download software, music, video, and documents. Lime Wire and Gnutella are examples
of P2P applications. Likewise, a P2P network consists of a collection of computers (or nodes)
that simultaneously act as both the "client" and "server" in order to share computing
capabilities, such as exchanging data, sharing resources, directory services, and supporting
communications through instant messaging (IM) and real time collaboration tools.

J. **Personally Identifiable Information (PII)** is any information about a human being, living
or deceased, that is maintained by an agency and that permits identification of that individual
to be reasonably inferred by either direct or indirect means (such as in data mining). This
includes but is not limited to name, home address, Social Security number, driver’s license, State-issued identification number, birth date, place of birth, mother’s maiden name, biometric records, education, financial transactions, medical information, non-work telephone numbers, criminal or employment history, and any other personal information that is linked or linkable to an individual.

K. **Personally Owned Equipment (POE)** is any equipment, device, or software that you provide.

L. **Political Appointees** are agency employees that are appointed by the President and confirmed by the United States Senate.

M. **Portable Electronic Devices (PEDs)** include personal digital assistants or PDAs, cell phones, smartphones, tablets, text messaging systems (e.g., BlackBerry), and plug-in and wireless peripherals that employ removable media (e.g., CDs, DVDs). PEDs also encompass USB flash memory (thumb) drives, external drives, and diskettes.

13. **References**

A. The Following references provide additional information on protecting agency system and information.


4. Office of Management and Budget (OMB) Circular A-130, Appendix III.

5. OMB M-07-16, Safeguarding and Responding to the Breach of Personally Identifiable Information.


7. DOT Order 1351.37 (as amended), Departmental Cybersecurity Policy.

8. DOT Order 1351.18 (as amended), DOT Privacy Risk Management Policy.

9. DOT Order 1351.33 (as amended), Departmental Web-based Interactive Technologies Policy (Social Media and Web 2.0).

10. FAA Order 1600.75, Protecting Sensitive Unclassified Information (SUI).


(13) FAA Human Resources Policy Manual (HRPM) ER-4.1, Standards of Conduct.
