National Aeronautics and Space Administration

Headquarters
Washington, DC 20546-0001

NASA Cybersecurity and Privacy Rules of Behavior

1. Introduction

A. The NASA Cybersecurity and Privacy Rules of Behavior (NASA ROB) provide the specific responsibilities and expected behavior for NASA systems and information users, as required by:
   (1) Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource, Appendix Ill, paragraph 3a(2)(a);*
   (2) NPD 2810*, NASA Information Security Policy*, and
   (3) NPD 2540, *Acceptable Use of Government Office Property Including Information Technology.*

B. All NASA information system users shall acknowledge and consent to the NASA ROB prior to being granted access to NASA systems, networks, applications or information, hereafter referred to as NASA Information Technology (NASA IT).

C. Authorized users must comply with the NASA ROB, using "due diligence" and maintain the highest ethical standards. NASA ROB do not supersede any federal or NASA policies that provide higher levels of protection to NASA's information or information systems.

D. Any account on any system provisioned by NASA for the user's official use shall be considered by the user as an authorized system and that they have authorized access.

E. NASA information system users **acknowledge and consent to the following terms and conditions** when accessing NASA IT:
   (1) You are accessing a U.S. Government (USG) information system (IS) that is provided for USG-authorized use only.
   (2) The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE) and counterintelligence (CI) investigations.
   (3) At any time, the USG may inspect and seize data stored on this IS.
   (4) Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception and search, and may be disclosed or used for any USG-authorized purpose.
   (5) This IS includes security measures (e.g., authentication and access controls) to protect USG interests.
   (6) All of the above conditions apply whether or not the access or use of an IS includes the display of a Notice and Consent Banner ("warning banner"). When a banner is used, the banner reminds the user of the NASA ROB, whether or not the banner describes these conditions in detail or in summary, and whether or not the banner expressly references the NASA ROB.

F. This acknowledgement and consent will be annually reaffirmed. Failure to do so shall result in the suspension or revocation of access to NASA IT.

G. Continued use of NASA IT without a current acknowledgement and consent does not relieve users from the obligations, responsibilities and penalties outlined in the NASA ROB.
H. Unauthorized or improper use of NASA IT may result in the suspension or revocation of access to NASA IT, and disciplinary action, as well as civil and criminal penalties.
I. . Examples of unauthorized or unapproved non-GFP include, but are not limited to, any device such as a mobile phone, tablet, computer, Internet of Things (IoT) device, or wearable technology that does not have a valid Authority To Operate (ATO) from a NASA Authorizing Official (AO), regardless of who provided or owns the device.
J. Any device without an approved ATO is considered an unauthorized device, regardless if it is 1) NASA owned and provided, 2) contractor owned, 3) other U.S. federal government owned, 4) foreign government owned, 5) grantee owned, 6) educational institution owned, or 7) personally owned.
   (1) Devices without NASA authorization can only access NASA Data or Services through a limited set of OCIO managed partner access services.
   (2) Devices identified as unauthorized must begin the process to become authorized and must be identified as part of an approved NASA contractor acquisition.

2. Applicability

These NASA ROB apply to all users accessing NASA IT resources, such as workstations, laptops, mobile devices, smartphones, applications, servers, networks, computers and to access, store, receive, or transmit NASA information, whether through authorized GFP, or approved/authorized non-GFP.

3. Applicable Documents

The following list contains documents that are incorporated by reference into the NASA ROB. NASA policy documents can be found at: https://nodis3.gsfc.nasa.gov/

(1) 5 U.S.C. § 552a, *Privacy Act of 1974*
(2) OMB Circular A-130, *Managing Information as a Strategic Resource*
(3) NPD 2810, *NASA Information Security Policy*
(4) NPD 2540, *Acceptable Personal Use of Government Office Property Including Information Technology*
(5) NPR 2810.1B, *Security of Information Technology*
(6) NPR 2190.1B: *NASA Export Control Program*
(7) NPR 2810.2, *Possession and Use of NASA Information and Information Systems Outside of the United States and United States Territories*
(8) NPR 3600.2A, *NASA Telework Program*
(9) NPR 2190.1B, *NASA Export Control Program*
(10) NASA Mobile Device Management (MDM) Personal Device Annual User Agreement and Authorization
(11) OCIO Policy Memorandum, *Use of Authorized Devices*, April 16, 2018
(12) Information Technology Security Handbook (ITS-HBK)-1382.09-01, *Privacy Rules of Behavior and Consequences: Overview*
(13) ITS-HBK-2810.09-02A, *NASA Information Security Incident Management*
(14) ITS-HBK-2810.15-02, *Access Control: Managed Elevated Privileges*

4. Protecting Sensitive Information

A. **User Requirements: Users shall**:
   (1) Comply with ITS-HBK-1382.09-01 and:
      a. Comply with the Privacy Act of 1974 requirements.
      b. Protect Personally Identifiable Information (PII) from unauthorized disclosure, dissemination, modification, or destruction.
      c. Request and access only the PII that the user is authorized to access.
      d. Encrypt all Sensitive But Unclassified (SBU) data and/or PII that is transmitted and/or downloaded onto a GFP or approved/authorized non-GFP, including mobile devices, to include full disk encryption on the device.
      e. Follow the SBU/Controlled Unclassified Information (CUI) guidelines for handling PII, and follow the requirements/restrictions for putting PII and SBU/CUI on removable media.

B. NASA Export Control Program Requirements:
   (1) **Users shall** follow all policies and regulations associated with the NASA Export Control Program.
      a. The NASA Export Control Program is a NASA-wide system established to ensure that exports and transfers to foreign parties in the course of approved international activities are consistent with Export Administration Regulations (EAR), and the International Traffic in Arms Regulations (ITAR).
      b. It is NASA policy to ensure that exports and transfers of commodities, technical data, or software to foreign persons and foreign destinations are carried out in accordance with United States export control laws and regulations, and Federal and NASA policy. Relevant export control laws and regulations include EAR *15 C.F.R. Pts. 730-774*, ITAR, *22 C.F.R. Pts. 120-130*, and regulations governing Assistance to Foreign Atomic Energy Activities, *10 C.F.R. Pt. 810*.
      c. All NASA employees and contractors shall follow the rules governing export control as described in NPR 2190.1B, and consult with the appropriate Center Export Administrator as needed.

5. System and Data Access Protections

A. **User Requirements: Users shall**:
   (1) Comply with most current version of NPD 2540.
   (2) Only access those NASA IT systems required to perform official duties.
   (3) Use the NASA Visitor Network for non-NASA businesses and access this network using non-NASA assets.
   (4) Complete the mandatory Security and Privacy Awareness Training and all system-specific and role-specific required training.
   (5) Only use NASA-provided or NASA-approved GFP or non-GFP devices to connect to NASA systems and networks.
   (6) Only use Government FIPS 140-2 encryption external storage devices to store NASA data when connecting to NASA networks or devices.
   (7) Only use trusted and/or authorized removable media to store and process NASA data or access/connect to NASA systems and networks.
   (8) Follow NASA policy and ROB, prohibiting unauthorized software installation and/or use.

(9) Log off or lock systems and/or authorized GFPs or non-GFPs whenever leaving their work area or leaving them unattended.
(10) Power off laptops when being transported outside of NASA facilities, or when unattended outside of NASA facilities (e.g., locked in a hotel room during travel).

B. **User Prohibitions: Users shall not**:
(1) Change default security settings or alter the configuration on authorized GFP or any non-GFP, once approved and authorized for access to NASA IT networks, systems or information, unless approved and documented in the authorized System Security Plan.
(2) Download, copy or install unapproved or unauthorized software applications or data programs onto NASA-provided or NASA-approved GFP or non-GFP device.
(3) Participate in peer-to-peer (P2P) file sharing, on-line gaming or gambling, or cryptocurrency-mining activities using NASA-provided or NASA-approved GFP or non-GFP devices.
(4) Use unapproved or unauthorized personally owned device, or other non-GFP to access NASA information systems and networks or process and store NASA information.
(5) Connect your NASA-provided or NASA-approved GFP or non-GFP devices to the NASA network and to another network at the same time.
(6) View, print, or distribute pornographic materials, or other materials with offensive or graphic content, as described in NPD 2540.
(7) Engage in criminal, infamous, dishonest, immoral conduct, or other conduct prejudicial to the government while using government furnished IT equipment and resources.
(8) Attempt to access NASA systems or information without appropriate authorization.
(9) Send, copy, or forward any NASA information without appropriate authorization.
(10) Allow unauthorized persons to use or access NASA-provided or NASA-approved GFP or non-GFP devices while attached to or accessing NASA networks, systems, or applications, or when NASA data is stored on a non-GFP.
(11) Access, process, or store classified information on any system or equipment that is not authorized for such access, processing, or storage.
(12) Use NASA-provided or NASA-approved GFP or non-GFP devices to copy or distribute intellectual property – including music, software, documentation, and other copyrighted materials – without permission or license from the copyright owner.
(13) Use unapproved or unauthorized cloud services to process and store NASA information.

6. Passwords and Other Access Control Measures

A. **User Requirements: Users shall**:
(1) Protect any privileged and non-privileged passwords, Personal Identity Verification (PIV) cards, Personal Identification Numbers (PINs), password tokens (SecurID), and access numbers from unauthorized use, disclosure, or access.

B. **User Prohibitions: Users shall not**:
(1) Share passwords, PIV cards, password tokens, PINs, or access numbers.
(2) Bypass, stress, or test Information Assurance (IA) or Computer Network Defense (CND) mechanisms (e.g., Firewalls, Content Filters, Proxy Servers, Anti-Virus Programs).

(3) Introduce or use unauthorized software, firmware, or hardware on any NASA IT resource.
(4) Participate in or contribute to any activity resulting in a disruption or denial of service.
(5) Write, code, compile, store, transmit, transfer, or introduce malicious software, programs, or code.
(6) Export/transfer user authentication and/or device certifications to unauthorized devices.

7. Internet, Email, and Social Media Use

A. NASA-provided internet and email is for official use, with limited personal use permitted per NPD 2540.
B. The NASA Visitor Network is only used by non-NASA businesses and accessed by non-NASA assets. Access to this network is provided as a courtesy to NASA users with non-NASA devices, and may be limited or terminated without notice.
C. **User Requirements: Users shall**:
(1) Be alert and watchful for scams, phishing emails, and other social engineering activities and report any suspicious email communications to the NASA SOC (1-877-NASA-SOC or soc@nasa.gov).
(2) Use only NASA-approved non-GFP devices, with the approved NASA Mobile Device Management (MDM), installed on the device in order to access NASA email and calendar services.
(3) Follow guidance from the NASA Office of Communications and Chief Information Officer (CIO), when using official or sanctioned NASA social media accounts:
a. http://communications.nasa.gov/socialmedia/tools1
b. http://communications.nasa.gov/socialmedia/guidance-2012
c. https://inside.nasa.gov/ocio/information/social_media.html
D. **User Prohibitions: Users shall not**:
(1) Access the NASA Visitor Network with NASA-provided or NASA-approved GFP or non-GFP devices or systems that process or store NASA data.
(2) Use an unauthorized personally owned device (non-GFP) to access NASA email or calendar services without first installing the NASA approved MDM container or solution on such device, and acknowledging the terms and conditions associated with installation and/or use of the MDM container/solution.
(3) Bulk or auto-forward or route NASA email to any non-NASA email account or unauthorized email system.
(4) Use personal email accounts to conduct NASA business without explicit written and signed authorization from the applicable Center Chief Information Security Officer (CISO).
(5) Nothing in this NASA ROB limits the rights any employee may have under Title 5 U.S.C. or other government-wide statute or regulation.
(6) Use NASA IT systems or email accounts to conduct any form of personal for-profit services.
(7) Make any statements on personal social media accounts that may be misconstrued as being made in an official NASA capacity.
(8) Open unauthorized NASA accounts on social media or other internet-based services.

(9) Post any NASA information, documents, data, pictures, graphics, charts, etc., on external newsgroups, social media and/other types of third-party website applications, or other public forums without authority, including information which is at odds with NASA missions or positions. This includes any use that could create the perception that the communication was made in an official capacity as a federal government employee.

(10) Use NASA IT resources in any way that would reflect adversely on NASA. Such uses include pornography, chain letters, unofficial advertising, soliciting or selling except on authorized bulletin boards established for such use, violation of statute or regulation, inappropriately handled classified information, SBU/CUI and PII, and other uses that are incompatible with public service.

8. Teleworking Considerations

A. NASA telework rules and requirements are described in NPR 3600.2A.

B. NASA may terminate or suspend teleworking at any time for any reason. Users' supervisors may revoke their telework privilege for failure to comply with applicable telework agreements.

C. Users may connect their GFP to their personal home network to log on to the NASA network via Virtual Private Network (VPN). They may connect personal peripherals such as monitors, keyboards, mice, and printers to their GFP.

D. **User Requirements: Users shall**:

(1) Use only NASA-provided GFP and approved/authorized non-GFP to connect to the NASA network.

(2) Follow security practices that are equivalent to those required at their primary workplace,

(3) Protect the confidentiality of Government information when using remote access.

E. **User Prohibitions: Users shall not**:

(1) Connect GFP or approved/authorized non-GFP to other networks while connected directly to the NASA network through means including wired Ethernet, wireless (Wi-Fi), USB, Bluetooth, cellular, or other technology.

(2) Connect unauthorized Universal Serial Bus (USB) portable media/storage to a NASA information system, including personally purchased thumb drives not authorized by NASA.

(3) Connect GFP or approved/authorized non-GFP to untrusted wireless networks without using NASA's provided VPN capability.

(4) Process or store SBU/CUI, PII, and other sensitive NASA information on non-GFP without signed authorization from the applicable CISO and Center Privacy Manager.

(5) Download files or attachments on public non-GFP (e.g., computers in a hotel business center, library, or internet cafe).

(6) Print emails or non-public Agency information in public areas or from public non-GFP printers.

9. Foreign Travel with IT

A. **User Requirements: Users shall**:
   (1) Adhere to the requirements set forth in NPR 2190.1C, NASA Export Control Program, and NPR 2810.2, Possession and Use of NASA Information and Information Systems Outside of the United States and United States Territories.
   (2) Use NASA GFP or approved/authorized non-GFP that meet the standards and conditions to store, process, transmit, and access NASA information as authorized for use on international travel.
   (3) Ensure that all NASA GFP or approved/authorized non-GFP remain in their possession or are appropriately safeguarded while outside the U.S. and U.S. territories.

B. **User Prohibitions: Users shall not**:
   (1) Use non-GFP for the conduct of NASA business while on foreign travel unless no other viable option is available and such use is authorized and approved by the Center CIO.
   (2) Open the NASA MDM container or solution from any non-GFP to access NASA email or calendar services while outside of the United States and its territories.

10. Incident Reporting

A. **User Requirements: Users shall**:
   (1) Follow the instructions in ITS-HBK-2810.09-02A when reporting an incident.
   (2) Immediately report IT security incidents or privacy breaches to NASA's SOC (1-877-NASA-SEC or soc@nasa.gov).
      a. Report the loss, damage, or theft of a NASA GFP or non-GFP that contains or may contain NASA SBU/CUI or PII data within **one** hour of knowledge of the loss, damage, or theft.
      b. Report the loss, damage, or theft of a NASA GFP or non-GFP that does not contain NASA SBU/CUI or PII data within **24** hours of knowledge of the loss, damage, or theft.
      c. Report suspected or confirmed loss of control over PII or unauthorized disclosures of PII immediately upon knowledge of the incident.

11. Rules of Behavior for System Administrator and Privileged Account Users

A. **NASA Privileged Account User Requirements: Privileged users shall**:
   (1) Comply with all system and network administrator responsibilities.
   (2) Use privileged accounts for official and authorized administrative actions only.
   (3) Complete all specialized role-based training, including annual refresher training.

B. **NASA Privileged Account User Prohibitions: Privileged users shall not**:
   (1) Install or remove any system hardware or software, or modify any system setting, that you are not authorized to change.
   (2) Give anyone, including yourself, privileges or access greater than is necessary to accomplish assigned roles and responsibilities.
   (3) Delete or modify audit logs, or prevent the auditing of privileged actions.
   (4) 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 information system).

(5) Use a privileged account to access the internet, unless in the required performance of duties.

12. Personally Owned Electronic Device Usage

A. **User requirements: Users shall**:
   (1) Have an approved, valid Authority to Operate (ATO) from a NASA Authorizing Official (AO) prior to the authorized use of non-GFP to store, process, or transmit NASA data or connection of such device to a NASA internal or non-public system and/or network.
   (2) Use the NASA MDM container or solution on authorized non-GFP for the purpose of accessing NASA email and calendar services.

B. **User Prohibitions: Users shall not use an unauthorized/unapproved non-GFP to**:
   (1) Connect to any NASA internal and/or non-public network (e.g., intranet) or system that contains anything other than publically available data.
   (2) Connect to any NASA IT device via USB, Bluetooth, or other communication channels.
   (3) Obtain a local Internet protocol address on the NASA internal network.
   (4) Access the NASA e-mail system, including Outlook Web Access.
   (5) Use or store NASA authentication credentials either directly on or by the unauthorized device or within applications on the unauthorized device.
   (6) Connect to non-public NASA services or any NASA service requiring user authentication.
   (7) Access resources via any NASA VPN system and/or any other remote access service.
   (8) Access, download, process, store, or transport NASA-owned or controlled data of any kind, including but not limited to, the user's government e-mail and cloud based systems.

I acknowledge that I have read, I understand, and I agree to comply with all the terms and conditions set forth in these aforementioned Rules of Behavior.

_____ _____

Name Date