April 18, 2024

NASA Cybersecurity and Privacy Rules of Behavior

1. General

a. These Rules of Behavior (RoB) apply to all NASA personnel (employees, contractors, interns, etc.) and any other individuals who are granted access to NASA information resources, networks, and Information Technology (IT) systems.

b. NASA Information Technology (NASA IT) includes all Federal Information Systems that contain or process NASA information, including operational technology and mission systems. Information systems are defined by 40 U.S.C. §11101 and include any equipment or interconnected system or subsystem of equipment used in the acquisition, storage, analysis, evaluation, manipulation, management, control, display, switching, interchange or transmission of data or information. NASA IT includes computers, ancillary and peripheral equipment, software, firmware, and physical devices.

c. For the purpose of this document, NASA's information systems include but are not limited to (1) this computer, (2) this computer network, (3) all computers connected to this network, and (4) all devices (e.g., iPhone, Android Smart Phone, etc.) and storage media (e.g., thumb drive, flash drive, etc.) attached to this network or to a computer on this network.

d. The NASA Chief Information Officer may authorize deviations from specific provisions of the NASA ROB when there is a documented need to accomplish Agency missions. Authorized deviations shall be made available in writing.

2. No Expectation of Privacy

By signing this document, I recognize and agree to the following:

a. I will not be granted access to NASA information resources, networks, and Information Technology (IT) systems unless I first read, acknowledge, consent to, and sign this document.

b. I must reaffirm this acknowledgement, consent to, and sign the latest NASA RoB annually. If I fail to reaffirm, my access to NASA IT resources may be suspended or revoked.

c. My continued use of NASA information or NASA IT without a current acknowledgement and consent does not relieve me from the obligations, responsibilities, and penalties outlined in the latest version of this document.

d. I shall comply with the NASA RoB, using "due diligence" and maintain the highest ethical standards. NASA RoB do not supersede any applicable federal or NASA policies that provide higher levels of protection to NASA's information or information systems.

e. That any NASA IT account on any system provisioned for my official use shall be considered an authorized system and that I have authorized access as a result.

f. That Information Systems (IS) include security measures (e.g., authentication and access controls) to protect USG interests.

g. That the above condition applies whether the access or use of an IS includes the display of a Notice and Consent Banner ("warning banner"). The banner is a reminder of the NASA RoB, whether it describes these conditions in detail or in summary, and whether the banner expressly references the NASA RoB or not.

h. I am accessing a U.S. Government information system that is provided for U.S. Government-authorized use and limited acceptable personal use in keeping with NPD 2540.

i. That I may be subject to disciplinary or other personnel action based on my employer's responsibilities under applicable contract, law, policies, and procedures, as well as civil and criminal penalties for any unauthorized or improper use of NASA IT, NASA information, or a NASA information system. Nothing in this document limits the rights I may have under Title 5 U.S.C. or other government-wide statute or regulation.

j. The Government, acting directly or through its contractors, routinely monitors communications occurring on the NASA network or NASA information systems. ***I have no reasonable expectation of privacy regarding any communications or data transiting, stored on, or traveling to or from any NASA information system.*** At any time, the government may for any lawful government purpose monitor, intercept, search, and seize any communication or data transiting, stored on, or traveling to or from any NASA information system.

k. Any communications or data transiting, stored on, or traveling to or from any NASA information system may be disclosed or used for any lawful government purposes.

l. Any device without an approved ATO is considered an unauthorized device, whether it is 1) NASA owned or leased 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 shall be identified as part of an approved NASA contract acquisition, agreement, or grant, and shall begin the process to become authorized.

3. Protecting Sensitive Information

When using and accessing NASA information and IT resources, I understand that I must comply with all documents specified in the Basis and Applicable Documents section below and:

a. Protect Personally Identifiable Information (PII) from unauthorized disclosure, dissemination, modification, or destruction.

b. Request and access only the PII that I am authorized to access.

c. Encrypt all Controlled Unclassified Information (CUI) and/or PII that is transmitted and/or downloaded onto GFP or approved/authorized non-GFP, including mobile devices, to include full disk encryption on the device. Remove any such data when no longer necessary at the user level.

d. Follow NASA CUI directives, including those concerning handling PII, and abide by NASA directives regarding the storage of PII and CUI on removable media.

e. Ensure proper disposition and/or sanitization of any non-electronic or electronic mechanism under my control containing privacy information, as outlined in *ITS-HBK-2810.11-02, Media Protection and Sanitization* and sensitive information (e.g., CUI) policy.

f. Be aware of the consequences of violations of NASA policy and federal requirements regarding the handling of PII as set forth in Appendix A.

4. Export Control Program Requirements

a. The NASA Export Control Program is a NASA-wide system established to ensure that exports and transfers to foreign parties during approved international activities are consistent with Export Administration Regulations (EAR), 15 C.F.R. Pts. 730-774, the International Traffic in Arms Regulations (ITAR), 22 C.F.R. Pts. 120-130, and regulations governing Assistance to Foreign Atomic Energy Activities, 10 C.F.R. Pt. 810.

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.

c. When dealing with Export Controlled Information and IT systems that store or manage this data, I recognize that I must:

   (1) Follow all policies and regulations associated with the NASA Export Control Program.

   (2) Follow the rules governing export control as described in NPR 2190.1B NASA Export Control Program and consult with the appropriate Export Administrator as needed.

5. Passwords and Other Access Control Measures

When using and accessing NASA information and IT resources, I understand that I must:

a. 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. Not share passwords, PIV cards, password tokens, PINs, or access numbers.

c. Not bypass, stress, or test Information Assurance (IA) or Computer Network Defense (CND) mechanisms (e.g., Firewalls, Content Filters, Proxy Servers, Anti-Virus Programs).

d. Not participate in or contribute to any activity resulting in a disruption or denial of service.

e. Not export/transfer user authentication and/or device certifications to unauthorized devices.

6. Incident Reporting

a. I understand that I must comply with the following requirements related to incident reporting.

b. Follow the instructions in ITS-HBK-2810.09-02 when reporting an incident.

c. Immediately report IT security incidents and all suspected or confirmed loss of control over PII or unauthorized disclosures of PII to NASA's SOC (1-877-NASA-SEC or soc@nasa.gov). Contractor shall report such incidents pursuant to paragraph B.

d. Report the loss, damage, or theft of NASA GFP or non-GFP that contains or may contain NASA CUI or PII data within **one** hour of knowledge of the loss, damage, or theft.

e. Report the loss, damage, or theft of NASA GFP or non-GFP that does not contain NASA CUI or PII data within 24 hours of knowledge of the loss, damage, or theft.

f. Report suspected or confirmed loss of control over PII or unauthorized disclosures of PII immediately upon knowledge of the incident.

g. *Please check if you are a Jet Propulsion Laboratory (JPL) employee.*

☐ As a user of Jet Propulsion Laboratory, I recognize my responsibility to report incidents to the JPL SOC according to local user guidance agreed to between NASA and the contractor operating the JPL FFRDC.

7. Internet, Email and Social Media Use

a. When using the Internet, Email, and/or Social Media, I understand that I must:

b. Only use NASA-provided internet and email for official use, with limited personal use permitted per NPD 2540.

c. Only use the NASA Visitor Network with my non-NASA devices that do not process or store NASA data and not use this network for official NASA business. The NASA Visitor Network is intended to be used by non-NASA businesses/users 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.

d. Be alert for scams, phishing emails, and other social engineering activities, and report any suspicious email communications to the NASA Security Operations Center (SOC). JPL employees should report any suspicious email communication to the JPL SOC.

e. Use only NASA-approved non-GFP, with the approved NASA Mobile Device Management (MDM) solution(s) installed on the device to access NASA email and calendar services.

f. Follow guidance from the NASA Office of Communications and Chief Information Officer (CIO), when using official or sanctioned NASA social media accounts:

(1) http://communications.nasa.gov/socialmedia/tools1

(2) http://communications.nasa.gov/socialmedia/guidance-2012

g. Not bulk or auto-forward or route NASA email to any non-NASA email account or unauthorized email system.

h. Not use personal email accounts to conduct NASA business without explicit written and signed authorization from the applicable Center Chief Information Security Officer (CISO). I shall obtain authorization from the Senior Agency Information Security Officer if I am not associated with a NASA Center.

i. Not use NASA IT or email accounts to conduct any form of personal for-profit services.

j. Never use my NASA-provided identifiers (e.g., email addresses) or authentication secrets (e.g., passwords/PINs) for creating accounts on external sites/applications.

k. Not open unauthorized NASA accounts on social media or other internet-based services.

l. Not post any non-public NASA information, documents, data, pictures, graphics, charts, etc., on external newsgroups, social media, generative AI, 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.

m. Not 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 handling classified information, CUI, or PII, and other uses that are incompatible with public service.

8. Teleworking Considerations

a. NASA telework rules and requirements applicable to civil servants are described in NPR 3600.2.

b. When teleworking, I may connect my GFP to my personal home network to log on to the NASA network via Virtual Private Network (VPN). I may connect personal peripherals to my GFP that do not provide data storage such as a monitor, keyboard, mouse, scanner, printer, home network router, headset (or any handsfree audio device), headphones, speakers, docking station, and webcam.

c. When teleworking, I recognize that I must:

(1) Use only Government-provided GFP or authorized non-GFP to connect to the NASA VPN.

(2) Follow security practices that are equivalent to those required at my primary workplace.

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

(4) Not connect GFP or approved/authorized non-GFP to other networks while connected directly to the NASA VPN through means including wired Ethernet, wireless (Wi-Fi), USB, Bluetooth, cellular, or other technology.

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

(6) Not connect GFP or approved/authorized non-GFP to untrusted wireless networks without using NASA’s provided VPN capability.

(7) Not download files or attachments that contain non-public NASA information on public non-GFP (e.g., computers in a hotel business center, library, or internet cafe).

(8) Not print emails or non-public NASA information in public areas or from public printers.

9. Foreign Travel with IT

When I go on Foreign Travel with NASA provided IT, I recognize that I must:

a. Adhere to the requirements set forth in NPR 2190.1, 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 (or any NID that modifies these NPRs).

b. 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.

c. Ensure that all NASA GFP or approved/authorized non-GFP remain in my possession or are appropriately safeguarded while outside the United States and United States Territories.

d. Not 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 my Center CIO. If I am not associated with a NASA Center, authorization shall be obtained from the Agency Office of the Chief Information Officer.

e. Not open the NASA MDM solution(s) from any non-GFP to access NASA email or calendar services while outside of the United States and United States Territories.

10. Expectations for System Administrators and Privileged Account Users

When utilizing system administrator or privileged accounts, I recognize my responsibility to:

a. Comply with all system and network administrator responsibilities.

b. Use privileged accounts for official and authorized administrative actions only.

c. Complete all specialized role-based training, including annual refresher training.

d. Not install or remove any system hardware or software, or modify any system setting, that I am not authorized to change.

e. Not give anyone, including myself, privileges or access greater than is necessary to accomplish assigned roles and responsibilities.

f. Not delete or modify audit logs or prevent the auditing of privileged actions.

g. Not 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).

h. Not use a privileged account to access the internet, unless in the required performance of duties.

11. Personally Owned Electronic Device Usage

When using Personally Owned Electronic Devices, I recognize that I must:

a. Have an approved, valid Authority to Operate (ATO) from a NASA Authorizing Official (AO) prior to the 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.

b. Use the NASA MDM solution(s) on authorized non-GFP for the purpose of accessing NASA email and calendar services.

c. Not connect to any NASA internal and/or non-public network (e.g., intranet) or system that contains anything other than publicly available data.

d. Not connect to any NASA IT device via USB, Bluetooth, or other communication channels.

e. Not obtain a local Internet protocol address on the NASA internal network.

f. Not access the NASA e-mail system, including Outlook Web Access.

g. Not use or store NASA authentication credentials (Example: user account and password) either directly on or by the unauthorized device or within applications on the unauthorized device.

h. Not connect to non-public NASA services or any NASA service requiring user authentication.

i. Not access resources via any NASA VPN system and/or any other remote access service.

j. Not 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.

12. System and Data Access

When using and accessing NASA information and IT resources, I understand that I must:

a. Comply with most current version of NPD 2540.

b. Only access NASA IT and information resources required to perform official duties.

c. Use the NASA Visitor Network only for non-NASA businesses and access this network only using non-NASA assets.

d. Complete the mandatory Security and Privacy Awareness Training and all system-specific and role-specific required training before gaining access to NASA information and information systems.

   (1) Complete yearly, mandatory refresher Cybersecurity and Privacy Awareness Training and all yearly system-specific and role-specific required training.

   (2) Only use NASA authorized devices to connect to NASA systems and networks. Use of non-GFP on NASA networks shall not be attempted unless specifically authorized by OCIO prior to connection to NASA systems and networks.

   (3) Only use NASA-approved encryption external storage devices to store NASA data when connecting to NASA networks or devices.

(4) Only use trusted and/or authorized removable media to store and process NASA data or access/connect to NASA systems and networks.

(5) Refrain from installing unauthorized software on NASA information systems or using unauthorized software to process NASA information.

(6) Log off or lock systems by removing and safeguarding my PIV whenever leaving my work area or leaving my system unattended.

(7) 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).

(8) Not 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.

e. Not download, copy, or install unapproved or unauthorized software applications or data programs onto NASA-provided or NASA-approved GFP.

(1) Not participate in peer-to-peer (P2P) file sharing, on-line gaming or gambling, or cryptocurrency-mining activities using NASA-provided or NASA-approved GFP.

(2) Not use unapproved or unauthorized personally owned device, or other non-GFP to access NASA information systems and networks or process and store NASA information.

(3) Not connect my NASA-provided or NASA-approved GFP or non-GFP to the NASA network and to another network at the same time.

(4) Not view, print, or distribute pornographic materials, or other materials with offensive or graphic content while using government furnished IT equipment and resources, as described in NPD 2540.

(5) Not engage in criminal, infamous, dishonest, immoral conduct, or other conduct prejudicial to the government while using government furnished IT equipment and resources.

(6) Not attempt to access NASA systems or information without authorization.

(7) Not send, copy, or forward any NASA information without authorization.

(8) Not allow unauthorized persons to use or access NASA-provided or NASA-approved GFP or non-GFP while attached to or accessing NASA networks, systems, or applications, or when NASA data is stored on non-GFP.

(9) Not access, process, or store classified information on any system or equipment that is not authorized for such access, processing, or storage.

(10) Not use NASA-provided or NASA-approved GFP to copy or distribute intellectual property – including music, software, documentation, and other copyrighted materials – without permission or license from the copyright owner.

(11) Not use unapproved or unauthorized cloud services to process and/or store NASA information.

13. Basis and Applicable Documents

a. These NASA RoB are based on federal guidance and are developed and updated in response to the ever-changing nature of IT and cyber security in the federal government.

b. These NASA Cybersecurity and Privacy Rules of Behavior (NASA ROB) provide the specific responsibilities and expected behavior for users of all NASA Information and Information Technology Systems as required by:

(1) Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource, Appendix I, paragraph 4(h)(6)*;

(2) NPD 2810.1, NASA Information Security Policy;

(3) NPD 2540.1, Acceptable Use of Government Furnished Information Technology Equipment, Services and Resources;

(4) OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, and

(5) NPD 1382.17, NASA Privacy Policy.

c. The following list contains documents that are incorporated by reference into the NASA ROB. They apply to contractors to the extent specified by law, or as otherwise specified in the applicable contract.

(1) 5 U.S.C. § 552a, Privacy Act of 1974

(2) OMB Circular A-130, Managing Information as a Strategic Resource

(3) OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information

(4) NPD 2810.1, NASA Information Security Policy

(5) NPD 2540.1, Acceptable Use of Government Furnished Information Technology, Equipment, Services and Resources

(6) NPD 1382.17, NASA Privacy Policy

(7) NPR 2810.1, Security of Information and Information Systems

(8) NPR 2190.1, NASA Export Control Program

(9) NPR 2810.2, Possession and Use of NASA Information and Information Systems Outside of the United States and United States Territories

(10)NPR 2810.7, Controlled Unclassified Information

(11)NPR 1382.1, NASA Privacy Procedural Requirements

(12)NPR 3600.2, NASA Telework Program (Applicable to NASA Civil Servants only)

(13)NASA Mobile Device Management (MDM) Personal Device Annual User Agreement and Authorization

(14)OCIO Policy Memorandum, Use of Unauthorized Devices, April 16, 2018

(15)Information Technology Security Handbook (ITS-HBK)-1382.09-01, Privacy Rules of Behavior and Consequences: Overview

(16)ITS-HBK-2810.09-02, NASA Information Security Incident Management

(17)ITS-HBK-2810.15-02, Access Control: Managed Elevated Privileges

(18)ITS-HBK-2810.11-02, Media Protection and Sanitization

NASA policy documents can be found at: https://developer.nasa.gov/pages/CSPD/rules-of-behavior-document-access/.

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

_____

My Printed Name

_____

My Signature

_____

Date

Appendix A: PII Violation Penalties

	NPR 1382.1B Citation	Issue	Administrative Consequence
NASA Users, Managers, and Information Owners	§3.5.2.6 §1.2.2.13.a §6.3.2.6 §3.3.2.6 §3.3.2.5 §3.5.2.6.a.2 & 3	Knowingly failing to implement and maintain information security controls required for the protection of PII; exceeding authorized access to, or disclosure to unauthorized persons of, PII; or failing to immediately report any suspected or confirmed breach of PII, including loss of control or unauthorized disclosures of PII, as an Information Security incident to the SOC **OR** Failing to adequately instruct, train, or supervise employees in their privacy responsibilities. **OR** Failing to conduct required review PII (including SSNs) activities and reduce and/or eliminate unnecessary collections of PII.	Actions include: Additional desk side privacy training for the NASA User/Manager/IO and their supervisor.
NASA Users	§3.2.2.5.a §1.2.2.13.a	Failing to participate in mandatory privacy training prior to gaining access to NASA information and information systems, and yearly thereafter. **OR** Failing to participate in privacy role-based training.	**1st Offense**: Account access suspended until the course is taken. Manager notified. **2nd Offense**: Account access suspended until the course is taken. Center CIO and manager notified. **3rd + Offense**: Account access suspended until the course is taken. NASA CIO, Center CIO, and manager notified.
Information System Owners	§5.7.2.5.c §5.3.2.2	Failing to obtain Web Measurement and Customization Technology use waiver prior to use of the technology when collecting PII. OR Failing to comply with provisions of the Children's Online Privacy Protection Act (COPPA).	Website will be removed from live production environment. NASA CIO and Center CIO notified. Additional desk side privacy training with the ISO and their manager.

Information System Owners	§2.3.2.4.a §2.3.2.4.b §2.3.2.4.c §2.3.2.4.e	Failing to conduct and complete a Privacy Threshold Analysis (PTA) for the application, website, or information system. OR Failing to conduct and complete a Privacy Impact Assessment (PIA) for an application, website, or information system with Information in Identifiable Form (IIF) on members of the public or as required by the Paperwork Reduction Act (PRA). **OR** Failing to conduct and complete a re-evaluation of the PTA, or PIA, as appropriate, after significant modification. **OR** Failing to complete an annual review of the PIA to maintain accuracy.	1st Offense: The application, website, or information system cannot be in live production or is suspended until review is completed. Agency Privacy Manager is notified. Additional desk side privacy training with the ISO and their manager. **2nd Offense**: The application, website, or information system cannot be in live production or is suspended until review is completed. Center Chief Information Officer (CIO) is notified. Additional desk side privacy training with the ISO and their manager.
Information System Owners	§2.3.3.4.d	Failing to conduct a PIA prior to use of a Third-Party Website or Application.	**1st Offense:** The Third-Party Website or Application cannot be utilized. Additional desk side privacy training with the ISO and their manager. **2nd Offense:** The Third-Party Website or Application cannot be utilized. Center CIO is notified. Additional desk side privacy training with the ISO and their manager. **3rd + Offense**: The Third-Party Website or Application cannot be utilized. NASA CIO and Center CIO notified. Additional desk side privacy training with the ISO and their manager.
Information System Owners	§5.7.2.5.b §5.7.2.5.c	Failing to obtain Web Measurement and Customization Technology use waiver prior to use of the technology when collecting PII. **OR** Failing to provide clear and conspicuous notice of Web Measurement and Customization Technology use on the website utilizing the technology.	Web Measurement and Customization Technology use will be pulled until an appropriate waiver is approved or notice is provided. NASA CIO and Center CIO notified. Additional desk side privacy training with the ISO and their manager

The following violations may lead to consequences taken in the judicial system, rather than by NASA:

NASA Users	§3.5.2.6.b	Willful and intentional violations of the Privacy Act.	May be subject to criminal penalties, guilty of a misdemeanor and fined not more than $5,000
Information System Owners	§3.5.2.4.a	Willfully failing to meet publication requirements for Privacy Act System of Records (SOR).	May be subject to criminal penalties, guilty of a misdemeanor and fined not more than $5,000