NASA Interim Directive

NID 2540.138

Effective Date: August 18, 2021
Expiration Date: August 18, 2022

Subject: Acceptable Use of Government Furnished Information Technology Equipment, Services and Resources

Responsible Office: Office of the Chief Information Officer

1. POLICY

a. It is NASA policy to permit limited acceptable personal use of NASA Government furnished property (GFP), information technology (IT) equipment, services and resources for non-government purposes, when such use does not overburden any of the Agency's IT services and resources, and when access to these IT services and resources does not interfere with official Government business. Government furnished property includes NASA assets, including all devices and equipment. The intent of limited acceptable personal use is to provide a professional and supportive work environment while meeting taxpayer expectations that tax dollars be spent wisely. Acceptable personal use shall be limited to use that incurs no more than minimal additional expense to the Government in areas such as: communications infrastructure costs; use of consumables in limited amounts; general wear and tear on property; minimal data storage on storage devices; and, minimal impacts on NASA IT systems..

b. It is NASA policy to permit limited acceptable personal use of NASA GFP, IT equipment, services and resources to individuals during non-duty time of reasonable duration and frequency of use, including during official work breaks, and when the use does not:

(1) adversely affect the performance of official duties;

(2) result in the loss of an individual's productivity;

(3) pose a cybersecurity risk;

(4) violate applicable laws and regulations, or

(5) interfere with the official business or mission of NASA.

c. It is NASA policy that NASA GFP, IT equipment, services and resources shall not be used for downloading illegal, inappropriate, or unauthorized content and untrusted, unapproved, or malicious software applications or services. Use of NASA GFP, IT equipment, services or resources is prohibited for commercial purposes, "for profit" and "non-profit" activities, or in support of outside employment or business activity.

d. It is NASA policy that individuals have no expectation of privacy while using any NASA GFP, IT equipment, services or resources at any time, including (but not limited to) accessing the Internet, proxy-bypass services, or e-mail. Individuals have no expectation of privacy even during limited periods of personal use. Individuals also have no expectation of privacy even if using personal equipment, services, and applications while connected to NASA GFP, IT equipment or services.

e. It is NASA policy that non-compliance or unauthorized or improper use of NASA GFP, IT equipment, services or resources may result in the suspension or revocation of access to NASA products, networks and services, disciplinary action, as well as civil and criminal penalties. Unauthorized and improper use is described in Attachment C.

f. It is NASA policy that Authorizing Officials for mission systems may impose stricter security controls, user privacy controls, and restrict applications for their systems due to mission criticality or unique mission requirements.

g. It is NASA policy that this NASA Interim Directive (NID) in no way limits Agency employees' and contractors' use of NASA GFP, IT equipment, services and resources for official Government activities, nor limits the rights any employee may have under Government-wide statute or regulation.

h. It is NASA policy that the privilege to use NASA GFP, IT equipment, services and resources for non-government purposes may be revoked or limited at any time by Federal or Agency officials. NASA Centers and contractors may invoke more stringent policies or implementation guidance.

2. APPLICABILITY

a. This NID is applicable to NASA Headquarters and NASA Centers, including Component Facilities and Technical and Service Support Centers. This language applies to the Jet Propulsion Laboratory, a Federally Funded Research and Development Center (FFRDC), other contractors, authorized users, grant recipients, or parties to agreements only to the extent specified or referenced in the appropriate contracts, grants, or agreements.

b. In this NID, all mandatory actions (i.e., requirements) are denoted by statements containing the term "shall." The terms "may" or "can" denote discretionary privilege or permission, "should" denotes a good practice and is recommended, but not required, "will" denotes expected outcome, and "are/is" denotes descriptive material.

c. This NID applies to NASA Information Technology User acceptable use of NASA GFP, approved/authorized non-GFP, NASA IT equipment, services, resources, and personally owned IT devices (including Internet of Things (IoT) devices) when connected to NASA GFP, IT equipment, services, resources, and NASA data. Additional policies and procedures on contractor-accountable, NASA-owned and Center-accountable property can be found in Federal Acquisition Regulation (FAR), Government Property, 48 CFR pt. 45; NASA FAR Supplement, Government Property, 48 CFR 1800, pt. 1845; and the terms and conditions of individual contracts.

d. This NID does not apply to NASA public data that does not reside on a NASA system.

e. In this NID, all document citations are presumed to be the latest version unless otherwise noted.

3. AUTHORITY

a. Federal Information Security Modernization Act of 2014, 44 U.S.C. §3551.

b. Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems.

4. APPLICABLE DOCUMENTS AND FORMS

a. NASA Procedural Requirements (NPR) 2810.2, Possession and Use of NASA Information and Information Systems Outside of the United States and United States Territories.

b. Standards of Ethical Conduct for Employees of the Executive Branch, 5 CFR pt. 2635.

c. Federal Acquisition Regulation, Government Property, 48 CFR pt. 45.

d. NASA FAR Supplement, Government Property, 48 CFR pts 1800 and 1845.

e. NASA Advisory Implementing Instruction 1050-3B, NASA Partnerships Guide.

f. NASA IT Rules of Behavior, 10 Oct 2020

5. RESPONSIBILITY

a. The Office of the Chief Information Officer (OCIO) shall:

(1) Be responsible for implementation, management, and maintenance of this NID, and ensuring this policy is widely disseminated to all NASA Information Technology Users.

(2) Ensure the existence of appropriate controls, managed at the Agency level, together with procedures that ensure NASA Information Technology Users are aware of proper personal use of GFP and non-GFP (including personally owned devices) when connected to NASA networks, IT equipment and services; and are responsible for developing cost-effective controls for monitoring or preventing abnormal or inappropriate use. Controls to be considered for GFP include blocking of inappropriate web sites and phone numbers, flagging abnormal long distance or other phone charges, and monitoring network traffic for suspicious traffic or inappropriate use.

b. Information System Owners (ISOs):

(1) Shall ensure that current NASA interns, partners, grantees, and other users covered under Space Act Agreements or other official NASA agreements are knowledgeable of Federal and Agency policy before using U.S. Government property, data, and services.

(2) May authorize limited installation of software necessary for mission functions with the documented approval of the system Authorizing Official.

(3) Shall ensure that software authorized per 5.b(2) above:

(a) meets supply chain requirements;

(b) is licensed for NASA use; and

(c) is obtained from a safe and authorized source.

(4) Shall request limited installation of software necessary for mission functions, in coordination with the Center IT Asset Manager (ITAM). A list of ITAMs is available at: https://www.nssc.nasa.gov/elmt

c. Current NASA interns, partners, grantees, and other users covered under Space Act Agreements or other official NASA agreements may, if explicitly authorized by the applicable ISO, use NASA GFP, IT equipment and services consistent with their agreements.

d. Contracting Officers, as defined in Federal Acquisition Regulation 2.101, or Agreement Managers as defined in NASA Advisory Implementing Instruction 1050-3B:

(1) Shall ensure that contractors are informed of allowable uses of Government IT resources, approved/authorized non-GFP, and personally owned devices as a part of their introductory IT security training, orientation, or the implementation of this policy as part of a NASA contract.

(2) Shall ensure that contractors address allowable use of Government IT resources in System Security Plans (SSPs), IT Security Plans, and IT Security Management Plans.

(3) Shall ensure contractors who process, store, or transmit NASA information on approved/authorized non-GFP or personally owned devices, IT equipment, software, and media do so only when the contract under which they perform specifically establishes terms and conditions for such use, that appropriate approvals have been obtained, and that the contractor otherwise meets and complies with NASA security standards and policy.

e. Supervisors:

(1) Shall promote the allowable use of NASA GFP, IT equipment, services and resources.

(2) Shall pursue sanctions for misuse of NASA GFP, IT equipment, services or resources, including potential disciplinary action.

(3) Shall ensure NASA Information Technology Users taking NASA GFP or IT equipment outside the U.S., whether on official or personal travel, meet the requirements in NPR 2810.2, Possession and Use of NASA Information and Information Systems Outside of the United States and United States Territories.

(4) Shall ensure NASA Information Technology Users taking NASA GFP or IT equipment outside of the U.S. have export authorization. This includes validating that there is an official work requirement for the employee or contractor that necessitates exporting GFP or IT equipment in support of government business.

f. NASA Information Technology Users:

(1) Shall comply with the requirements regarding personal use of NASA GFP, IT equipment, services and resources and the Rules of Behavior for U.S. Government property, data, and services as outlined herein and in Attachments C (Specific Provisions) and G (Rules of Behavior) to this directive.

(2) Are responsible for knowing that they have no expectation of privacy while using any NASA GFP, IT equipment, services or resources at any time, including, but not limited to, accessing the Internet, proxy-bypass services, or e-mail, even during limited periods of personal use.

(3) Are responsible for knowing that they have no expectation of privacy while using personal equipment, services, and applications while connected to NASA GFP, IT equipment, services or resources.

(4) To the extent that they are civil servants, shall ensure that the personal use is consistent with Standards of Ethical Conduct for Employees of the Executive Branch, 5 CFR pt. 2635.

(5) Shall conduct themselves professionally in the workplace and not use NASA GFP, IT equipment and services for activities that are inappropriate or illegal.

(6) Shall ensure that the personal use of NASA GFP, IT equipment, services or resources does not create the appearance that they are acting in an official capacity or that NASA endorses or sanctions any personal activities.

(7) Shall distinguish between official and personal communications to ensure that all official communications are identified and conducted in conformance with applicable law, regulation, and policy.

(8) When using NASA GFP, IT equipment, services or resources, shall use social media in a responsible, safe, and judicious manner, whether in an official capacity or for personal use, which protects mission objectives, information assets, program integrity, data, and NASA's reputation.

(9) Shall not alter or change in any way configurations for NASA GFP, IT equipment, services or resources in a manner that does not adhere to NASA policy, specifications, or standards.

(10) Shall not use NASA GFP, IT equipment, services or resources to download illegal, inappropriate, or unauthorized content or untrusted, unapproved, or malicious software applications or services.

(11) Shall not use NASA GFP, IT equipment, services or resources for commercial purposes, “for profit” and “non-profit” activities, or in support of outside employment or business activity, such as a sole proprietorship.

(12) Shall not download, copy, or install unapproved or unauthorized software applications or data programs onto NASA GFP, IT equipment, services or resources, or NASA-approved and authorized networks and devices, including, but not limited to:

(a) screen savers

(b) computer games

(c) personal financial management software

(d) tax preparation software

(e) free, test, trial, or demo software

(f) “push” technology applications

(g) network monitoring software

(h) video-conferencing software

(i) Virtual Machines (VMs)

(13) Shall not engage in other prohibited activities on NASA GFP, IT equipment, services or resources or NASA-approved and authorized networks and devices, including, but not limited to:

(a) peer-to-peer (P2P) file sharing

(b) online file storage using services not explicitly authorized by NASA

(c) online gaming or gambling

(d) cryptocurrency-mining

(e) Installing, viewing, or accessing the following types of software or websites:

(i) Pornographic, sexually explicit, or sexually oriented materials.

(ii) Personal services websites, such as dating services where a user registers using NASA credentials and creates an appearance that the user is acting in an official capacity or that NASA endorses/sanctions the activity.

(iii) Hacking-related websites or sites which expose NASA to unacceptable security risk regardless of the known or potential security risks or lack thereof.

(iv) Proxy-bypass services, or services of similar capabilities such as those in Attachment E.

(v) Unauthorized remote access sites or software, or services of similar capabilities such as those in Attachment E.

(14) Shall not install software created or maintained by companies banned by the Federal Government on NASA GFP, IT equipment, services or resources, or on any system storing, transmitting or processing NASA data. See Attachment F.

(15) Shall not connect by any method equipment manufactured by companies banned by the Federal Government to NASA GFP, IT equipment, services or resources, or on any system storing, transmitting or processing NASA data. See Attachment F.

(16) Shall not use equipment manufactured by companies banned by the Federal Government for any government or non-government business use including but not limited to: hardware, telecommunications, data storage, data processing, or video or voice communications. This prohibition applies to:

(a) All business uses and business infrastructure, including those not tied to the Government or Government data.

(b) Any and all Bring Your Own Device (BYOD) programs; meaning all banned equipment shall not participate in any contractor BYOD programs.

(c) All contractor IT equipment, services, or resources including corporate, visitor, test, stage, production, stand-alone; prohibited telecommunications equipment shall not connect to any contractor-owned, managed, or out-sourced network or system.

(d) Connecting any contractor IT equipment, services or resources to any equipment, personally owned or otherwise, that uses or is equipment banned by the Federal Government.

(17) While physically on a NASA center, facility, campus or any type of NASA property shall only connect any personal device, used wholly and entirely for personal use, which is manufactured by a company banned by the Federal Government, to non-government commercial cellular services.

(18) Shall access the NASA Visitor Network:

(a) only for non-NASA purposes; and

(b) only using NASA Domain Name System (DNS) servers; and

(c) only using Hypertext Transfer Protocol (HTTP)/HTTP over Transport Layer Security (HTTPS) applications.

(19) Shall not access the NASA Visitor Network using NASA GFP or IT equipment.

(20) Shall not use personally owned equipment to access NASA GFP, IT equipment, services or resources except as explicitly authorized by the NASA CIO, e.g., authorized personal mobile devices under Mobile Device Management (MDM).

(21) Shall not connect unauthorized non-NASA devices to NASA GFP, IT equipment, services or resources via Universal Serial Bus (USB), Bluetooth, or any other connection methods.

(22) Shall not connect NASA GFP, IT equipment, services or resources via any method to any non-NASA GFP or IT equipment that provides data storage. This includes but is not limited to: USB or "thumb drive" external storage devices, external hard drives, smart phones, tablets and cameras.

(23) May, during situations that require conducting government business at a remote location, connect NASA GFP and IT equipment that has been assigned to them to the following acceptable personally owned non-NASA devices through wired or wireless connections, if such equipment is not manufactured by companies banned by the federal government (see Attachment F).

(a) A personally owned monitor

(b) A personally owned keyboard

(c) A personally owned mouse

(d) A personally owned scanner

(e) A personally owned printer

(f) A personally owned home network router

(g) A personally owned headset or handsfree audio device

(h) Personally owned headphones

(i) A personally owned webcam

(24) Shall remove NASA GFP or IT equipment from the workplace only to support official business.

(25) Shall ensure that NASA GFP or IT equipment outside of the workplace is used in support of official business, and such GFP or IT equipment:

(a) Remains in their custody;

(b) Is handled and maintained properly; and

(c) Is returned in good condition.

(26) Shall notify their supervisor, the NASA Security Operations Center (SOC) at soc@nasa.gov or 877-NASASEC (877-627-2732), and their respective Center Physical Security office as soon as possible if NASA GFP or IT equipment is lost, stolen or damaged.

6. DELEGATION OF AUTHORITY

None.

7. MEASUREMENT/VERIFICATION

ISOs may access any electronic communications conducted via NASA GFP and IT equipment and services and employ monitoring tools to detect improper use in accordance with U.S. law. ISOs or their designees determine, implement, ensure, and document compliance by applying a verification approach that is tailored to meet the requirements of this NID. The Office of Protective Services (OPS) conducts functional reviews, spot checks, and inspections to review compliance and implementation. The ISO employs enterprise tools on their systems to detect unauthorized access.

8. CANCELLATION

NPD 2540.1I, Personal Use of Government Office Equipment Including Information Technology, August 19, 2019.

ATTACHMENT A. DEFINITIONS

“Authorization to Operate”is the formal acceptance, by an Authorizing Official, that the security of an information system’s operation is commensurate with the risk and magnitude of harm resulting from a compromise of that system’s confidentiality, integrity, and availability.

“Authorizing Official” is a senior Federal official or executive with the authority to authorize (i.e., assume responsibility for) the operation of an information system or the use of a designated set of common controls at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation.

“Government furnished property” is property owned or leased by the Federal Government and includes Government office property that is property in the possession of, or directly acquired by, the Government and can be subsequently furnished to the contractor for performance of a contract.

“Government furnished property” also includes contractor-acquired property, if the contractor-acquired property is a deliverable under a cost contract when accepted by the Government for continued use under the contract. (Federal Acquisition Regulation, Part 45.101) This also includes property provided for use while in official travel status or provided for telework or other alternative workspace arrangements.

Government furnished property includes, but is not limited to:

a. computers and related peripheral property

b. software

c. library resources

d. research or reference services (e.g., online journals)

e. telephones and wireless communications devices (e.g., cell phones, smartphones, pagers)

f. personal electronic devices (e.g., calculators, music players, global positioning system devices, book readers)

g. facsimile machines

h. photocopiers

i. office supplies

j. Government guest networks

k. network access (e.g., Internet, wireless, cellular)

l. e-mail

m. licenses (e.g., software licenses)

"Information System Owner," per NPR 1382.1, NASA Privacy Procedural Requirements, means the principal advisor to the Center Chief Information Security Officer (CISO) on matters pertaining to specific information systems.

"Information Technology" is any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data by the Agency. This includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

"Information Technology User" is any employee, contractor employee, or any other individual authorized to access or use NASA Information Technology.

"NASA Information" per NPD 2810.1, NASA Information Security Policy, means any knowledge that can be communicated regardless of its physical form or characteristics, which is owned by, produced by or for, or is under the control of NASA.

"Network" means a system implemented with a collection of connected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

"Personally owned device" includes but is not limited to any device such as a phone, tablet, laptop, personal computer, Internet of Things device, or wearable technology that does not have a valid Authorization to Operate (ATO) from a NASA Authorizing Official (AO).

"Personal use" means other than for official Government business.

"Peer-to-Peer file sharing," as defined in OMB M-04-26, Personal Use Policies and "File Sharing" Technology, refers to any software or system allowing individual users of the internet to connect to each other and trade files.

"Privilege" means, in the context of this policy, that NASA is extending the opportunity to its Information Technology Users to use GFP for limited personal use to create a more supportive work environment. NASA Information Technology Users have no inherent right to personal use or ownership of GFP. The personal use privilege does not extend to modifying GFP, including modifications such as loading personal software or making configuration changes, or other changes that are inconsistent with Agency policy.

"Property" means a tangible asset, end item, or nonexpendable property that is functionally complete, not intended for sale, does not lose its identity, or become a component part of another item when put into use. Property is not intended to be destroyed during an experiment and has a useful life of two years or more.

“Proxy-Bypass Service” is a service used to bypass specific cybersecurity elements implemented in firewalls and proxies by bypassing security controls used to restrict or manage access. Any attempt to bypass security protocols is prohibited.

“Push Technology” is a style of internet-based communication where the request for a given transaction is initiated by the publisher or central server. A user "subscribes" to various information "channels" provided by a server; whenever new content is available on one of those channels, the server pushes that information directly to the user’s system without any request action being taken by the user.

"Social media" includes, but is not limited to, wikis, blogs, mash-ups, Web feeds (e.g., Really Simple Syndication and Rich Site Summary (RSS) feeds), social networking sites (e.g., Facebook), microblogging (e.g., Twitter), and Web-based forums.

“Unapproved or Unauthorized Software or Services” are applications and IT services that do not have a NASA Authorization to Operate or have been approved for use by NASA. This includes FedRAMP services that have not completed the NASA Assessment and Authorization process.

ATTACHMENT B. ACRONYMS

AO	Authorizing Official
ATO	Authorization to Operate
BYOD	Bring Your Own Device
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISO	(Center) Chief Information Security Officer
DNS	Domain Name System
E.O.	Executive Order
FAR	Federal Acquisition Regulation
FedRAMP	Federal Risk and Authorization Management Program
FFRDC	Federally Funded Research and Development Center
FIPS	Federal Information Processing Standards
GFP	Government Furnished Property
HBK	Handbook
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over Transport Layer Security
IoT	Internet of Things
ISO	Information System Owner
IT	Information Technology
ITAM	(Center) IT Asset Manager
ITS	Information Technology Security
MDM	Mobile Device Management
NASA	National Aeronautics and Space Administration
NID	NASA Interim Directive
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
OCIO	Office of the Chief Information Officer
OMB	Office of Management and Budget
OPS	Office of Protective Services

P2P	Peer-to-Peer
SOC	Security Operations Center
SOP	Standard Operating Procedure
SSP	System Security Plan
TIC	Trusted Internet Connection
USB	Universal Serial Bus
U.S.C.	United States Code
VM	Virtual Machine
VNC	Virtual Network Computing
VPN	Virtual Private Network

ATTACHMENT C. SPECIFIC PROVISIONS

C.1. Employees and contractors are permitted limited personal use of GFP and IT services to the extent that such personal use does not interfere with official duties or result in a loss of productivity and for contractors only to the extent specified or referenced in the appropriate contracts. Employees and contractors are only authorized to use office property and services for personal use if they are first authorized to use the property for official business. NASA is not required to supply property if the property is not required for the employee or contractor to perform official business. Moreover, personal use may incur only minimal additional expense to the Government in areas such as:

a. Communications infrastructure costs such as, but not limited to, telephone or data charges, Internet connectivity, and telecommunications traffic.

b. Consumables such as, but not limited to, paper, ink, and toner.

c. Wear and tear on property such as, but not limited to, copiers and printers.

d. Impacts to network bandwidth such as, but not limited to, e-mail message sizes, e-mails with attachments, text messaging and personal use of social media (e.g., Twitter, Facebook, YouTube).

C.2. Inappropriate Personal Use - Employees and contractors are expected to conduct themselves professionally in the workplace and to refrain from using GFP and IT services for activities that are inappropriate. Misuse or inappropriate use of GFP and IT services includes, but is not limited to:

a. Any personal use that violates applicable law, regulation, Federal or Agency policies, or procedural requirements.

b. Any personal use of unauthorized streaming media services (or other software or services that could cause unnecessary congestion, delay, or disruption of service to any Government system or component). Examples include, but are not limited to, Netflix, SiriusXM, Amazon Prime Video/Music, Pandora, Spotify, Disney+, YouTube TV, or any other similar services.

c. Using a Government system as a staging ground or platform to gain unauthorized access to other systems.

d. The creation, copying, transmission, or retransmission of unauthorized mass mailings, regardless of subject matter.

e. Activities inconsistent with the Standards of Ethical Conduct for Employees of the Executive Branch 5 CFR pt. 2635.

f. Accessing, sharing, posting, storing, or copying material that is inappropriate or offensive based on race, color, national origin, sex, religion, age, disability, genetic information, sexual orientation, gender identity, or status as a parent.

g. Creating, searching/downloading, viewing, storing, copying, or transmitting materials describing or depicting sexually explicit conduct, or other sexually explicit or sexually oriented materials.

h. Use for commercial purposes, "for profit" activities, or in support of outside employment or business activity such as a personal business, or assisting friends, relatives, or others in such activities (e.g., consulting for pay, sales, or administration of business transactions, and sale of goods or services, unless on authorized bulletin boards provided by the Agency).

i. Engaging, in a personal or private capacity, in any outside fundraising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any partisan political activity (e.g., expressing opinions about candidates, distributing campaign literature).

j. Publicly communicating Agency information, including Agency policy, project, or program information and other critical data, that does not concern a protected disclosure under Title 5, United States Code (Government Organization and Employees), or that has not been authorized for release. This includes uses that could create the perception that the communication was made on behalf of the Agency or the Office of the Administrator if the communication has not been authorized by the Office of Communications. Authorized public communications of Agency information are subject to Release of Information to News and Information Media, 14 CFR pt. 1213, and applicable Agency policies.

k. Any use that could generate more than minimal additional expense to the Government.

l. The unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information, including computer software and data, that includes privacy, copyrighted, trademarked information, or material with other intellectual property rights (such as literature, music, and videos beyond fair use), proprietary data, or export controlled software or data.

m. Participation in P2P file sharing activities or use of such software including, but not limited to, BitTorrent, uTorrent, Gnutella, and Vuze.

n. Overriding or defeating a security feature of a Government system (e.g., installing unapproved software or jailbreaking).

C.3. Privacy Expectations - NASA employees and contractors do not have a right to expect privacy while using Government office property or IT services at any time, including accessing the internet and using email. Employees and contractors are advised that the Government maintains call detail and network access records to monitor telephone activity and internet access and employs monitoring tools to track system performance and improper use. To the extent that employees and contractors wish their private activities to remain private, they must avoid personal use of GFP and IT services. By using GFP, employees and contractors consent to disclosing the contents of any files or information maintained on or passed through the property. Any use of Government communication resources is made with the understanding that such use is subject to Government surveillance and inspection in accordance with the law, is not private, and is not anonymous. This includes personal property (e.g., tablets, smartphones) that connect to Government networks and services.

C.4. Sanctions for Misuse - Unauthorized or improper use of GFP and IT services could result in loss of use or limitations on the use of property, disciplinary or adverse personnel actions, criminal penalties, and/or employees/contractors being held financially liable for the cost of improper use.

ATTACHMENT D. REFERENCES

D.1. Government Organizations and Employees, Title 5, United States Code.

D.2. The Hatch Act, 5 U.S.C. § 7323.

D.3. Definitions, 40 U.S.C. § 11101(6).

D.4. Principles of Ethical Conduct for Government Officers and Employees. Executive Order (E.O.) 12674 of April 12, 1989, as amended by E.O. 12731 of October 17, 1990.

D.5. Federal Information Technology, E.O. 13011 of July 16, 1996, as amended by E.O. 13284 of January 23, 2003, and E.O. 13286 of February 28, 2003.

D.6. Release of Information to News and Information Media, 14 CFR, pt. 1213.

D.7. Office of Personnel Management, Employee Responsibilities and Conduct, 5 CFR pt. 735.

D.8. Supplemental Standards of Ethical Conduct for Employees of the National Aeronautics and Space Administration, 5 CFR pt. 6900.

D.9. Federal Acquisition Regulation, Government Property, 48 CFR pt. 45.

D.10. NASA FAR Supplement, Government Property, 48 CFR 1800 pt. 1845.

D.11. OMB M-04-26, Personal Use Policies and "File Sharing" Technology.

D.12. OMB M-10-23, Guidance for Agency Use of Third-Party Websites and Applications.

D.13. OMB M-13-10, Antideficiency Act Implications of Certain Online Terms of Service Agreements.

D.14. NPD 1900.9, Ethics Program Management.

D.15. NPD 2810.1, NASA Information Security Policy.

D.16. NPR 1382.1, NASA Privacy Procedural Requirements.

D.17. NPR 1900.3, Ethics Program Management.

D.18. NPR 2810.1, Security of Information Technology.

D.19. NPR 2810.2, Possession and Use of NASA Information and Information Systems Outside of the United States and United States Territories.

D.20. NPR 3600.2, NASA Telework Program.

D.21. NPR 4200.1, NASA Equipment Management Procedural Requirements.

D.22. NASA Information Technology Security Handbook (ITS-HBK) 2810.07-01, Configuration Management.

D.23. ITS-HBK-2810.15-01, Access Control.

D.24. ITS-HBK-2810.17-01, Identification and Authentication.

D.25. NASA ITS-SOP 2810.01A, Collection of Electronic Data.

ATTACHMENT E. EXAMPLES

E.1. Examples of Proxy-Bypass Services: 3Proxy, Unblockme, and Proxite.

E.2. Examples of unauthorized remote access protocols, sites, or software: Telnet, VNC, X11 (when configured to allow remote access), LogMeIn, TeamViewer, Chrome Remote Desktop, GoToMyPC, Apple Remote Desktop, BeAnywhere, ShowMyPC, and any non-NASA issued VPN software.

ATTACHMENT F. BANNED COMPANIES

F.1. Federal Agencies are prohibited from procuring video and telecommunication equipment from two People's Republic of China telecommunications companies, including their subsidiaries and affiliates:

a. Huawei Technologies Company; and

b. ZTE Corporation.

F.2. Federal Agencies are also prohibited from procuring certain video surveillance products or telecommunications equipment and services produced or provided by three People's Republic of China companies (or any subsidiary or affiliate of those entities):

a. Hytera Communications Corporation;

b. Hangzhou Hikvision Digital Technology Company; and

c. Dahua Technology Company.

F.3. Additionally, Federal Agencies are prohibited from using any hardware, software, or services developed or provided, in whole or in part, by:

a. Kaspersky Lab (or any successor entity);

b. Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or

c. Any entity of which Kaspersky Lab has majority ownership.

ATTACHMENT G. RULES OF BEHAVIOR

NASA Cybersecurity and Privacy Rules of Behavior (10 Oct 2020)

1. Introduction

A. The NASA Cybersecurity and Privacy Rules of Behavior (NASA ROB) provide the specific responsibilities and expected behavior for users of all NASA Information Technology Systems 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 Furnished Information Technology Equipment and Resources.*

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 U.S. Federal Code 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 include computers, ancillary and peripheral equipment, software, firmware, and physical devices.

C. All NASA IT users shall acknowledge and consent to the NASA ROB prior to being granted access to NASA IT or information resources.

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 in writing.

E. Authorized users 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.

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

G. Users of NASA IT **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.

H. NASA requires those with access to NASA IT to reaffirm this acknowledgement and consent annually. User failure to reaffirm shall result in the suspension or revocation of access to NASA IT.

I. 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.

J. Examples of unauthorized or unapproved non-Government furnished property (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), regardless of who provided or owns the device.

K. Unauthorized or improper use of NASA IT may result in the suspension or revocation of access to NASA IT, disciplinary action, and/or civil and criminal penalties. For contractors, such disciplinary or other personnel action is the responsibility of their employers under applicable law, policies and procedures.

L. Any device without an approved ATO is considered an unauthorized device, regardless of 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.

M. Users will be held responsible for the compromise of NASA information through negligence or a willful act.

N. 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.

2. Applicability

These NASA ROB apply to all users accessing NASA IT and information resources, such as workstations, laptops, mobile devices, smartphones, applications, servers, networks, computers, and to their efforts to access, store, receive, or transmit NASA information, whether through authorized GFP, or approved/authorized non-GFP. These NASA ROB apply to contractors only to the extent specified in the applicable contract.

3. Applicable Documents

The following list contains documents that are incorporated by reference into the NASA ROB. These documents apply to contractors to the extent specified by law, or as otherwise specified in the applicable contract. 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 Use of Government Furnished Information Technology Equipment and Resources*
(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* (Applicable to NASA Civil Servants only)

(9) NASA Mobile Device Management (MDM) Personal Device Annual User Agreement and Authorization
(10) OCIO Policy Memorandum, *Use of Authorized Devices*, April 16, 2018
(11) Information Technology Security Handbook (ITS-HBK)-1382.09-01, *Privacy Rules of Behavior and Consequences: Overview*
(12) ITS-HBK-2810.09-02A, *NASA Information Security Incident Management*
(13) 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 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, to include 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 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 NASA IT and information resources 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 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.

(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 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.
(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.
(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 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 authorization.
(9) Send, copy, or forward any NASA information without authorization.
(10) 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.
(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 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) Participate in or contribute to any activity resulting in a disruption or denial of service.
(4) Export/transfer user authentication and/or device certifications to unauthorized devices.

7. Incident Reporting

A. **User Requirements: Users (with the singular exception of Jet Propulsion Laboratory (JPL) FFRDC users) shall**:
   (1) Follow the instructions in ITS-HBK-2810.09-02 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). Contractor shall report such incidents pursuant to paragraph B.
      a. Report the loss, damage, or theft of 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 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.

B. Users of JPL FFRDC NASA IT shall report incidents to the JPL SOC according to local user guidance agreed to between NASA and the contractor operating the JPL FFRDC.

8. 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 Security Operations Center (SOC). Contractor employees should report any suspicious activity on NASA IT to the appropriate NASA SOC.
   (2) Use only NASA-approved non-GFP, 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). If the user is not associated with a NASA Center, authorization shall be obtained from the Senior Agency Information Security Officer.
   (5) Use NASA IT or email accounts to conduct any form of personal for-profit services.
   (6) Make any statements on personal social media accounts that may be misconstrued as being made in an official NASA capacity.
   (7) Open unauthorized NASA accounts on social media or other internet-based services.

(8) Post any non-public 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.

(9) 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.

9. Teleworking Considerations

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

B. NASA may terminate or suspend teleworking for civil servants 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). Users may connect personal peripherals to their 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.

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

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

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

10. Foreign Travel with IT

A. **User Requirements: Users shall**:

(1) 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.

(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 United States and United States 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. If the

user is not associated with a NASA Center, authorization shall be obtained from the Agency Office of the Chief Information Officer.

(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 United States Territories.

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 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

(URL for Graphic)

None

Distribution

NODIS