SUBJECT: Security of Information Technology
Responsible Office: Office of Chief Information Officer

1. POLICY
It is the policy of NASA Langley Research Center (LaRC) to:

a. Comply with NASA and Federal regulations on prohibited use of Information Technology (IT) resources.

b. Ensure IT resources are used only for official Government business, emergencies, or authorized personal use. Use of the NASA Internet address space “nasa.gov” is a representation of the Agency analogous to the use of NASA letterhead in which the opinions expressed reflect on NASA. As set forth below, limited personal use of IT resources owned by or operated on behalf of LaRC is considered to be an “authorized use” of those resources.

(1) IT resources owned by or operated on behalf of LaRC are provided for official business. Official Government business broadly includes any computer processing and communications that are required as part of the job. Official business includes, but is not limited to, the performance of NASA work-related duties in position descriptions, professional training and class work, work covered under grant agreements with NASA, tasks directed via NASA contracts, agreements with international partners, and support activities related to NASA contract tasking which include laboratory computer systems.

(2) LaRC management considers certain other activities to be within the scope of official business. For example, electronic mail or Web sites being used to distribute information about the following:

(a) Work-related events, such as technical symposiums, classes, and presentations.
(b) Activities sponsored by LaRC, such as the child care center and carpooling.
(c) Events and activities specific to a particular LaRC organization.
(d) LaRC-sanctioned activities, such as blood drives, clubs, and organizations.

(3) If there is no measurable additional cost, some limited personal use of Internet services is permitted provided it does not interfere with employee work or the work of others and does not put Agency systems or information at risk. Extreme care must be taken regarding the content accessed. Use must be kept to brief periods when it can reasonably be assumed that the employee is in a non-duty status, such as during lunch breaks. However, extensive personal Internet access during work hours utilizing Government resources is not appropriate.
(4) Under no circumstances is it permissible to intentionally access, download, or send material in any format that relates to hate, racism, or sexuality that would create a hostile or offensive work environment.

(5) Limited personal use of Government telephones and electronic mail is authorized as designated in NASA Policy Directive (NPD) 2540.1, Personal Use of Government Office Equipment Including Information Technology. However, extensive personal use of Government resources is not appropriate.

(6) Use caution regarding the disclosure of information within social network arenas. It is inappropriate to release non-public information without advance approval or to jeopardize your safety or the safety of others by divulging private or privileged information.

(7) Any external or non-NASA system containing or processing NASA data is required to obtain an external NASA security plan known as an “Authorization to Operate”. This will require the submission of a system security plan compliant with FISMA requirements based on NIST SP 800-53 Rev4, or NIST SP 800-171. It is the responsibility of the contractor to provide evidence of a satisfactory independent assessment of the submitted system security plan.

(8) All contractors, grantees, and any other entity requiring access to the NASA VPN is required to have a NASA Authorization to Operate or approved interconnection agreement.

c. Use IT resources owned by or operated on behalf of LaRC along with associated information in a responsible manner so as not to place other IT resources at risk. Users of NASA Langley IT resources shall:

(1) Be authorized and sponsored by a LaRC organization.

(2) Use the NASA Operational Messaging and Directory (NOMAD) system, the official NASA electronic mail system, for electronic mail service.

(3) Select and use unique, strong passwords.

(a) Refer to the current NASA prescribed version of NIST SP 800-53 for password formulation details.

(b) Passwords should not contain information about their owners, such as name, family information, work information, or other personal information.

(c) Passwords shall not be shared with anyone.

(d) Passwords shall not be written down on or posted on the asset the password is protecting.

(e) Passwords shall be protected from any form of disclosure to include, but not limited to, the following: stored in clear-text files; saved in function keys; and remembered by applications such as terminal logins, electronic mail clients or

Verify correct version before use by checking the LMS Web site.
web browsers.

(f) Passwords shall not be transmitted over the internet using insecure methods. Wherever possible, security protocols including IMAPS, FTPS, HTTPS, etc. shall be used.

(g) Password managers are not approved for use on NASA systems.

(4) Report any computer vulnerabilities, incidents of possible misuse, or suspected unauthorized access to line managers, system administrators, or the LaRC Chief Information Security Officer (CISO). Report all suspected IT security (ITS) incidents or possible inappropriate use immediately by telephone to the NASA Security Operations Center (SOC) 1-877-NASA-SEC or locally at extension 44200. (See Information Security Handbook, ITS-HBK-2810- 09-01, Incident Response and Management: NASA Information Security Incident Management)

(5) Follow NASA guidelines for handling and protection of Sensitive But Unclassified (SBU) data (see NPR 1600.1, NASA Security Program Procedural Requirements) to include, but not limited to:

(a) Mark “SENSITIVE BUT UNCLASSIFIED” at the top and bottom of the first page and each page containing SBU information. Cover SBU document with completed NASA Form (NF) 1686.

(b) Ensure “need to know” is applicable prior to release of SBU data. Do not release SBU data to Foreign Nationals. Ensure NF 1737 is signed prior to release of SBU data. If disposing of paper SBU documents, use a cross-cut shredder to render the printed information unreadable.

(c) Lock SBU documents away when unattended (including those on laptops and portable media).

(d) Encrypt all portable devices containing SBU data. Encrypt SBU data when transmitting. SBU is required to be encrypted in transit with approved encryption protocols. Print SBU material only if “secure print” option is available. Do not leave SBU data unattended.

(6) Utilize a temporary, travel, or loaner computer when going on international travel whether the international travel is of a personal or official nature. Exceptions to this policy based on specific mission requirements may be approved by LaRC IT Security.

(a) Upon return from travel, the temporary/loaner computer should be properly wiped and sanitized before use by another user.

(7) Do not divulge protected Personally Identifiable Information (PII) such as, but not limited to, Social Security numbers or an individual’s name in combination with any one or more of the following associated pieces of information: date and place of birth, mother’s maiden name, driver’s license number, passport number, financial account numbers, credit card numbers, financial records, medical records, criminal records, employment performance information.
d. Prohibit the following activities without the explicit written permission of the LaRC CISO or OCIO:

(1) Utilizing Internet protocol (IP) addresses for a device on LaRCNet that has not been assigned by the OCIO.

(2) Using a single IP address for multiple computers. For example, using network address translation or port address translation (NAT/PAT).

(3) Connecting IT resources that are not Government-owned to LaRCNet, except for IT resources owned and operated by support personnel. Using personal devices connected to LaRCNet is prohibited except when connecting to the Center VPN system or to the Center guest network.

(4) Connecting, other than by the Information Technology Infrastructure Branch any network communications devices to LaRCNet, including, but not limited to: routers, switches, hubs, concentrators, firewalls, virtual private networks, modems, encryption devices, or wireless access points.

(5) Connecting any IT resource on LaRCNet to any external network through a direct physical, wireless, or modem connection.

(6) Executing any program to analyze network traffic, except by personnel who are responsible for the maintenance and/or security of LaRCNet.

(7) Downloading, installing, or executing software without ITAM approval, this is inclusive of freeware, shareware and open source software.

(8) Storing any NASA information on unapproved non-NASA online storage facilities without concurrence by the LaRC CIO.

(9) Utilizing cloud provided services including software as a service, infrastructure as a service or platform as a service for NASA business without that service possessing a NASA ATO or exception approved by the CISO and center CIO.

(10) Connecting any IT resource to any internal Langley Network without ensuring that it meets the minimal ITS standards by having the system scanned by Langley IT Security for vulnerabilities. Vulnerabilities discovered by the scan shall be corrected or mitigated before the system is utilized in production.

(11) Connecting any personally owned devices to NASA Langley internal networks, whether the network is wired, wireless or a VPN connection.

(12) Connecting personally owned removable media to NASA Langley systems.

(13) Connecting NASA owned media to systems that do not have a NASA authorization to operate (ATO).

(14) Establishing any domain or other centrally managed authentication mechanisms without the explicit written approval of the LaRC CIO.
(15) Operation of any mobile WiFi hotspot device without concurrence by the LaRC Chief Information Security Officer.

(16) Downloading, installing, or executing any peer-to-peer file sharing software without concurrence by the LaRC Chief Information Security Officer.

(17) Granting foreign nationals or foreign representative accounts on IT resources owned by or operated on behalf of LaRC without concurrence by the LaRC Chief Information Security Officer and Chief of Security. (See NPR 1600.1A, NASA Security Program Procedural Requirements.)

(18) Downloading, exchanging, or copying any copyrighted works for which licensing has not been acquired.

e. Protect NASA information against accidental leakage in accordance with the requirements of the National Institute of Standards and Technology (see NIST SP800-88). Any electronic storage device that has ever contained NASA information, even for a brief period of time, must be sanitized before it can be reassigned, transferred, or discarded. (See ITS-HBK 0035, Digital Media Sanitation.)

f. Non-compliance with this LAPD may result in a charge to the organization for restoration of service, a loss of access to LaRC IT resources, disciplinary actions or criminal prosecution.

g. All NASA and support personnel shall be individually responsible and accountable for proper and legal use of IT resources owned by, or operated on behalf of, the U.S. Government. All NASA and support personnel are collectively responsible for protecting public confidence and financial investment in NASA.
2. **DEFINITIONS**

   a. **NASA Data** - information that is not approved for public release and is in an electronic format that allows it to be retrieved or transmitted.

   b. **IT System** - 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 or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources. (Reference NIST SP800-53 Rev. 4, 40 U.S.C. Sec 1401)

3. **APPLICABILITY**

   a. This LAPD applies to all LaRC employees and support personnel authorized access to IT resources that are owned by or operated on behalf of LaRC.

   b. In this directive, 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. In this directive, all document citations are assumed to be the latest version unless otherwise noted.

4. **AUTHORITY**

   a. National Aeronautics and Space Act of 1958

   b. NPD 2810.1, NASA Information Security Policy

5. **APPLICABLE DOCUMENTS**

   a. Title 18 U.S. Code, §1913, Lobbying With Appropriated Monies

   b. NPD 1440.6, NASA Records Management

   c. NPD 2540.1, Personal Use of Government Office Equipment Including Information Technology

   d. NPR 1600.1A, NASA Security Program Procedural Requirements

   e. NPR 2810.1, Security of Information Technology

   f. NPR 1441.1, NASA Records Management Program Requirements

   g. NRRS 1441.1, NASA Records Retention Schedules

   h. NASA-STD-2804, Minimum Office Automation Software Suite Interface

   i. ITS-HBK 0035, Digital Media Sanitation
j. ITS-HBK 902, Incident Response and Management: NASA Information Security Incident Management

k. NIST Computer Security Division Special Publications 800 Series

l. NASA Public Key Infrastructure Practices (http://pki.nasa.gov)

m. LAPD 2400.3, Langley Research Center (LaRC) Computer Networks for Data Communications

n. LPR 1440.7, Langley Research Center (LaRC) Records Management Procedural Requirements

o. LMS-CP-1725, Export Control

p. LMS-CP-2722, Property Disposal
6. **RESPONSIBILITY**

Specific responsibilities of individuals and organizations apply as specified in NPR 2810.1.

7. **DELEGATION OF AUTHORITY**

None

8. **MEASUREMENTS/VERIFICATION**

None

9. **CANCELLATION**


/s/ Cathy H. Mangum
Center Associate Director

DISTRIBUTION:
Approved for public release via the Langley Management System; distribution is unlimited.