



Responsible Office: Office of Chief Information Officer

SUBJECT: Security of Information Technology

1. POLICY

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

- a. Comply with NASA and Federal regulations on prohibited use of IT resources.
- b. Ensure that 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.
 - (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 daycare 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, 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 2540.1G "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 advanced approvals or to jeopardize your safety or the safety of others by divulging private or privileged information.

(7) The reception of commercial television broadcasts or other streaming media on the Government network without approval is not permitted.

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 IT resources connected to the LaRC network (LaRCNet) 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 NIST SP 800-53 Rev 3 for password formulation details.

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

(c) Passwords shall not be shared with anyone.

(d) 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 web browsers.

(e) Account lockout shall occur after five failed login (password entry) attempts if possible.

(f) Passwords shall not be transmitted in the clear.

(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 in a timely manner by telephone (extension 44200) or by encrypted electronic mail. (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 1686.
- (b) Ensure "need to know" is applicable prior to release of SBU data. Do not release SBU data to Foreign Nationals. Ensure NASA Form 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. Do not send SBU via personal email. Only print SBU if "secure print" option is available. Do not leave SBU data unattended.

(6) Do not divulge protected Personally Identifiable Information (PII) such as, but not limited to, social security numbers, an individual's name in combination with any one or more of the following associated pieces of information: data 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.

(7) Do not perform any moves, additions, alterations, or replacement of any LaRCNet connections, cable plant, or any other associated equipment. Associated equipment includes, but is not limited to: routers, switches, hubs, firewalls, virtual private networks, network intrusion detection systems, modems and wireless access points.

(8) Do not engage in inappropriate activities to:

- (a) Harass other users.
- (b) Degrade system or network performance.

- (c) Deprive authorized user access to an IT resource.
 - (d) Circumvent computer security measures.
 - (e) Access data or systems for which proper authorization has not been granted.
- (9) Do not engage in prohibited activities, to include but not be limited to:
- (a) Accessing, download, create, view, store or transmit material relating to gambling, illegal weapons, or terrorism.
 - (b) Outside or personal business activities.
 - (c) Fund raising, providing political endorsement, or lobbying.
 - (d) Unauthorized network traffic monitoring of any kind, or downloading, installing, or using security related programs or utilities to include, but not limited to: sniffers, scanners, or password crackers.
 - (e) Advertise goods or services for sale for monetary or personal gain.
 - (f) Send chain letters, personal mass mailings, hoaxes, or harassing messages.
 - (g) Unauthorized access to other computer systems or information, whether or not intentional.
- (10) Users should be particularly careful about using NASA computer systems in any way that could be interpreted as intending to influence any member of Congress to favor or oppose any legislation or appropriation. If the offender is an officer or employee of the United States, such an act may fall under a provision of Title 18 U. S. Code, Section 1913, "Lobbying with appropriated monies," which carries severe penalties upon conviction. If there are any questions about any aspect of this provision of law, contact the LaRC Office of Chief Counsel for advice and assistance.
- (a) Ensure all outgoing, reproduced, and distributed controlled information to include, but not limited to, electronic mail and file transfers to non-U.S. persons in the United States or abroad is authorized and complies with U.S. export control laws, regulations, and NASA export control policy (see LMS-CP-1725).
 - (b) Comply with NASA and Federal regulations to ensure adequate protective measures, risk analysis, risk assessments and IT system security plans are in place for all IT resources owned by or operated on behalf of LaRC.
 - (c) Ensure all IT resources connected to LaRCNet meet minimal ITS standards as defined by the LaRC CISO and LAPD 2400.3, "Langley Research Center (LaRC) Computer Networks for Data Communications" to include, but not be limited to:

- i. Displaying the official Government warning banner on all computers that connect directly to LaRCNet where operationally possible. That banner is: "WARNING! This U.S. Government computer is for authorized users only. By accessing this system you are consenting to complete monitoring with no expectation of privacy. Unauthorized access or use may subject you to disciplinary action and criminal prosecution."
- ii. Being assigned to an authorized IT system security plan.
- iii. Ensuring software, firmware, and operating system patches are installed on all devices prior to connection to LaRCNet and continually update patches in an expeditious manner or as directed by the LaRC Office of Chief Information Officer.
- iv. Maintaining current anti-virus software.
- v. Ensuring software packages required by the NASA or LaRC CIO are installed on all compatible systems, unless a written waiver request has been approved.
- vi. Ensuring all network capable devices are in compliance with NASA-STD-2804, unless a written waiver request has been approved.
- vii. Utilizing regular, periodic back-ups and periodic verification of the ability to restore files from back-ups.
- viii. Disabling the automatic start-up of network services that are not utilized.
- ix. Restricting access to the IT resources to the greatest extent possible to include, but not be limited to, the use of TCP wrappers on UNIX systems, access control lists, and elimination of default vendor accounts. However, devices shall be configured in a manner that allows LaRC IT Security scanning systems to monitor them for vulnerabilities.
- x. Restricting file sharing to the maximum extent possible. Users with a need to share files shall do so utilizing a file share server.
- xi. Enabling system logs, review logs weekly at a minimum for unauthorized access or suspicious activity, and store logs for one year. (Logs are official records and are maintained in accordance with LPR 1440.7, "Langley Research Center (LARC) Records Management Procedural Requirements.")
- xii. Using Government approved encryption software to protect administratively controlled information including, but not limited to, Privacy Act, export controlled, or proprietary while in transit over a network that includes back-up or archival storage.

d. Prohibit the following activities:

- (1) Connecting any IT resource to LaRCNet without ensuring that it meets the minimal ITS standards by having the system scanned for vulnerabilities. Vulnerabilities discovered by the scan shall be corrected or mitigated before the system is utilized in production.
- (2) Establishing any Microsoft Windows domain or other centrally managed authentication mechanisms without the explicit written approval of the LaRC CIO.
- (3) Operation of any mobile WiFi hotspot device within the LaRC campus.
- (4) Downloading, installing, or executing any peer-to-peer file sharing software.
- (5) 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 Officer and Chief of Security. (See NPR 1600.1, "NASA Security Program Procedural Requirements.")
- (6) Downloading, exchanging, or copying any copyrighted works for which licensing has not been acquired.

e. 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 LaRC contractors in support of NASA. 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 (see LAPD 2400.3, "Langley research Center (LaRC) Computer Networks for Data Communication"), 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 any freeware, shareware, public domain and/or commercial software from any foreign site, bulletin board, university, Internet service provider or any other non-commercial or non-U.S. Government site to include, but not limited to: software, music, and video without authorization.

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

f. Download and install software only if the software has been evaluated for correctness of execution and is available from NASA, another U.S. Government agency, or reputable commercial vendor site within the United States.

g. Comply with Agency PKI directives and usage instructions for encrypting NASA information resources (see <http://pki.nasa.gov>).

h. 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.)

i. 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.

j. All NASA and contractor employees 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 contractor employees are collectively responsible for protecting public confidence and financial investment in NASA.

2. APPLICABILITY

This LAPD applies to all LaRC employees, all LaRC contractor and subcontractor employees, and all other individuals authorized access to IT resources that are owned by or operated on behalf of LaRC.

3. AUTHORITY

- a. NPD 2810.1D, "NASA Information Security Policy"
- b. National Aeronautics and Space Act of 1958

4. APPLICABLE DOCUMENTS

- a. Title 18 U. S. Code, Section 1913, "Lobbying with appropriated monies"
- b. NPD 1440.6H, "NASA Records Management"

- c. NPD 2540.1 "Personal Use of Government Office Equipment Including Information Technology"
- d. NPR 1600.1, "NASA Security Program Procedural Requirements"
- e. NPR 2810.1, "Security of Information Technology"
- f. NPR 1441.1, "NASA Records Retention Schedules"
- g. NASA-STD-2804, "Minimum Office Automation Software Suite Interface"
- h. ITS-HBK 0035, "Digital Media Sanitation"
- i. ITS-HBK 902, "Incident Response and Management: NASA Information Security Incident Management"
- j. NIST Computer Security Division Special Publications 800 Series
- k. NASA Public Key Infrastructure Practices (<http://pki.nasa.gov>)
- l. X.509 Certificate Policy for National Aeronautics and Space Administration (NASA) Public Key Infrastructure (PKI)
- 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"
- q. LMS-CP-5630, "Requesting, Modifying, or Restoring a Public Key Infrastructure (PKI) Certificate"
- r. LMS-CP-5631, "Suspending or Revoking a Public Key Infrastructure (PKI) Certificate"

5. RESPONSIBILITY

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

6. DELEGATION OF AUTHORITY

None

7. MEASUREMENTS/VERIFICATION

None

8. CANCELLATION

LAPD 2810.1, Security of Information Technology, dated May 12, 2005

Original signed on file

Stephen G. Jurczyk
Deputy Director

DISTRIBUTION:

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