JPL Cybersecurity Requirements, Rev. 15

Document Owner: Robert L. Miller

Effective Date: August 21, 2017

Table of Contents

Introduction

Applicability

These cybersecurity requirements specify the minimum set of security requirements to be met by JPL employees for the protection of JPL systems processing unclassified data.

Background

JPL requires that unclassified JPL IT assets and data be protected from harm or loss. This harm or loss can be caused by the unavailability, unauthorized modification, and/or unauthorized disclosure of data or information that impacts JPL's missions, functions, and/or image. Measures must be taken at all levels of computer interaction to safeguard these assets from compromise.

The purpose of this document is to establish cybersecurity requirements that outline how JPL employees are to observe and implement protections for unclassified JPL computer systems, data, and information. These requirements apply to networked (including remote connections) and isolated IT equipment, applications, and users. The implementation of these requirements will provide protection from most threats while minimizing impact on computer system usability and efficiency. It should be recognized that these requirements are intended to mitigate risk identified by a general, Lab-wide risk assessment. Risks to individual project or program areas might be greater than the baseline risks that drive these requirements. Consequently, the line manager for each IT system may determine that additional cybersecurity controls are necessary based on the results of the risk analysis in the associated IT security plan.

This document specifically excludes security requirements for protecting classified data specified in contractual agreements with JPL, which may cover classified work. Information and guidance concerning the security the protection of classified data can be found by searching JPL Rules at https://rules.jpl.nasa.gov/ for "classified."

IT System Category

JPL IT Systems are categorized consistent with Federal Information Processing Standards (FIPS) publication FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*. The FIPS PUB 199 category is determined from some or all of the following:

- National Institute of Standards and Technology (NIST) Special Publication (SP) *800-60 Rev. 1, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories*
- National Institute of Standards and Technology (NIST) Special Publication (SP) *800-60 Rev. 1, Volume II: Appendices*
- The collection of JPL Information Categories identified in each IT System's inventory (described next)

Information Categories

All information stored, processed, or transmitted by JPL's information systems must be afforded the appropriate level of protection according to the risk and impact of the information being altered, destroyed, made unavailable, or disclosed. JPL has established six information categories for IT assets: High; Mission; Business and Restricted Technology; Scientific, Engineering, and Research; Administrative; and Public access. The information categories, inventory type, and isolation status determine the applicability of cybersecurity requirements.

The information categories have been combined into three groups that correspond to, and are consistent with, the High, Moderate, and Low security categories defined in FIPS PUB 199.

High Security Category

High Information Category

This category consists of information, software applications, and IT assets whose alteration, destruction, or unavailability could have a severe or catastrophic effect on JPL. The result could be severe degradation in, or loss of, JPL's capability to perform one or more primary mission functions; major damage to JPL assets; major financial loss; or severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

Moderate Security Category

Mission (MSN) Information Category

This category consists of information, software applications, and IT assets that support JPL's mission operations needs. Alteration, destruction, or unavailability of items in this category could have a serious adverse effect on JPL operations, assets, or individuals.

Business and Restricted Technology (BRT) Information Category

This category consists of information, software applications, and IT assets that support JPL's business or technological needs. Alteration, destruction, unavailability, or inappropriate disclosure of items in this category could have a serious adverse effect on JPL, e.g., non-compliance with laws and regulations; lawsuits and criminal prosecution against Caltech employees at JPL or JPL contractors; or the illegal export of technology.

The following is a list of example BRT information types:

- Restricted, unclassified information types found in Appendix 2 of "Marking and Handling Information" (JPL Rules! DocID 77806)
- Financial information
- Legal information
- Payroll information
- Personnel information
- Procurement information
- Source selection information
- Proprietary information entrusted to JPL
- Technical information controlled for export by U.S. Export Laws and Regulations
- Privacy information (defined in http://rules.jpl.nasa.gov/cgi/glossary2.pl?sl=P)
- Security plans
- Lists of vulnerabilities paired with property IDs, DNS hostnames or IP addresses

Low Security Category

Scientific, Engineering, and Research (SER) Information Category

This category consists of non-export-controlled information, software applications, and IT assets that support JPL's basic research, engineering, and technology development. Alteration, destruction, or unavailability of items in this category could have a limited adverse effect on JPL's research and development activities by causing unplanned expenses or schedule delays, but would not impede JPL's ability to achieve primary mission goals. SER information frequently resides on workstations used to perform scientific or engineering analyses or to develop software.

Integrity is the driving concern in this category followed by availability. Confidentiality is important and should be considered in a risk assessment insofar as it protects individual researchers from premature disclosure of their work. The impact, however, primarily affects the individual.

Administrative (ADM) Information Category
This category consists of information, software applications, and IT assets that support JPL's administrative IT systems. Alteration, destruction, or unavailability of items in this category could have a limited adverse effect on JPL by affecting the ability to conduct daily activities and use organization-run applications. ADM information typically includes routine office automation files stored on a user's computer.

Integrity and availability are the driving cybersecurity concerns. Confidentiality may be of concern in certain specific cases. In such instances, additional security controls must be imposed as a risk analysis dictates.

Public Access (PUB) Information Category
This category consists of information, software applications, and IT assets that support JPL's systems specifically intended for public use or disclosure. Alteration, destruction, or unavailability of items could have a limited adverse effect on JPL by exposing JPL to embarrassment, loss of credibility, or public ridicule. However, there would be little direct impact on JPL's missions.

Integrity and availability are the driving concerns. Cybersecurity controls are selected to protect the resources themselves and are not intended to protect the confidentiality of public information.

Security Control Families

The security requirements contained in this document are organized by control families established in the National Institute of Standards and Technology (NIST) document, *Special Publication (SP) 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, April 2013 (includes updates as of 01-15-2014).*

Table 1 lists general security control identifiers and family names.

TABLE 1: SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

Table J-1, also from NIST 800-53, Revision 4, lists supplemental privacy control identifiers by family.

TABLE J-1: SUMMARY OF PRIVACY CONTROLS BY FAMILY

ID	PRIVACY CONTROLS
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-6	Privacy Reporting
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal

TABLE J-1: SUMMARY OF PRIVACY CONTROLS BY FAMILY - CONTINUED

ID	PRIVACY CONTROLS
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Inventory Types
The requirements in this document apply to hardware, operating systems, middleware, and applications.

Property Types
Although all IT equipment, physical or virtual, can be considered to be some special-purpose form of computer, the JPL IT inventory is divided into several specific property types and subtypes. Some technical requirements are applicable to all property types, while others are only applicable to a subset of property types.

The categories of property types addressed by technical configuration requirements are:

- CPU – Laptop and desktop computers and virtual machines (including cloud instances)
- Mobile Device – Handheld computing device primarily with all of the following features:
  - Operated by a touchscreen
  - Uses a limited function operating system
  - Incapable of running a general-purpose operating system (Windows, MacOS, etc.)
- Network Printer
  - Includes networked copier machines
  - Excludes non-networked printers, e.g., connected by USB cables
- Network Component
  - Includes routers, switches, firewalls, gateways, bridges, load balancers, etc.
- Smartphone - Mobile phone with additional functionality including the ability to run applications
- Network Storage Device
- Limited Function Networked Device
  - Includes networked x-terminals, conference room projectors, HVAC controllers, badge readers, VOIP phones, etc.

Isolated is a characteristic of property records, applications, and cybersecurity requirements. An item is isolated if:

- It is air-gapped, or
- The JPL Cybersecurity/Identity Technologies & Operations Group determines that the item resides on a network whose architecture prevents communication with devices not residing on the network

This document distinguishes between two classes of isolated requirements. In the first class, selected requirements apply to the inventory types listed, whether the inventory item is isolated or not; in the second class, requirements apply only to selected isolated devices. These classes are designated by “Also Isolated” and “Only Isolated”, respectively.

Application Type

In addition to property, some applications must comply with the applicable requirements listed in this document. For security-planning purposes, ongoing risk assessment within JPL's risk management framework determines the types of applications that must be tracked in the Application Security Registry (ASR). The criteria for determining applicability are listed in http://cybersecurity.jpl.nasa.gov/appsec.php.

Appendix A of this document lists the subset of requirements that applies to applications.

Waivers and Liens

The requirements in this document are Category A requirements. The instructions for requesting waivers or liens are available from the ITSDB by clicking on Help at https://itsdb.jpl.nasa.gov/itsdb/. Cybersecurity liens have an expiration date, while waivers do not.

Note: The ITSDB is the institutional repository for all waivers and liens for requirements appearing in this document.

Document Organization and Usage

Each cybersecurity requirement is provided a unique identifier. The collection of requirements is organized by NIST 800-53 control family and then by each associated NIST security control. A requirement header has been added to improve readability.

Applicability of a requirement is indicated using one of two arrays of checkboxes. The first array type includes checkboxes related to affected information categories and inventory types, as shown in Figure 1.

When no inventory checkboxes are displayed, the requirement applies to every inventory type and/or user, depending on the information categories selected and the context of the requirement, as illustrated in Figure 2.

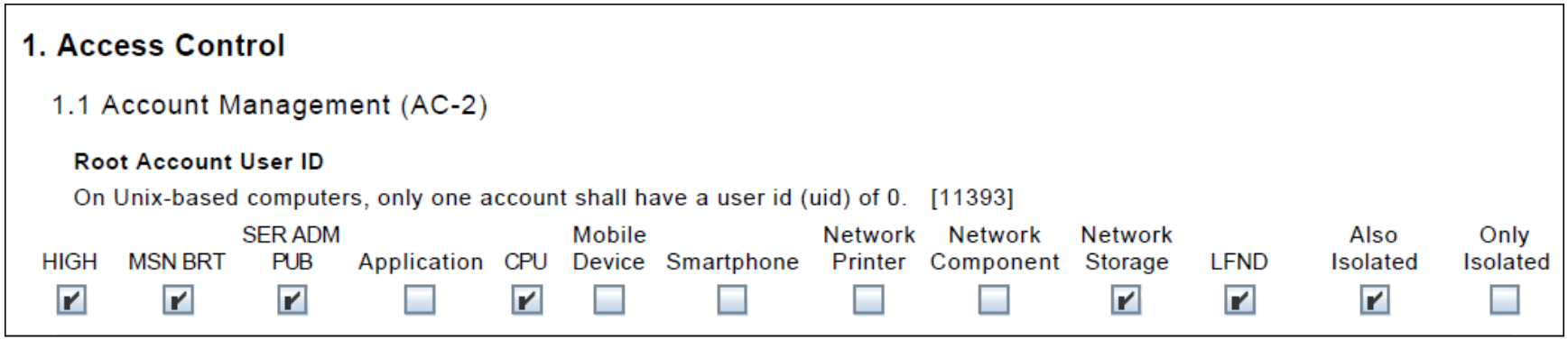

Figure 1: Requirement with Inventory Checkboxes

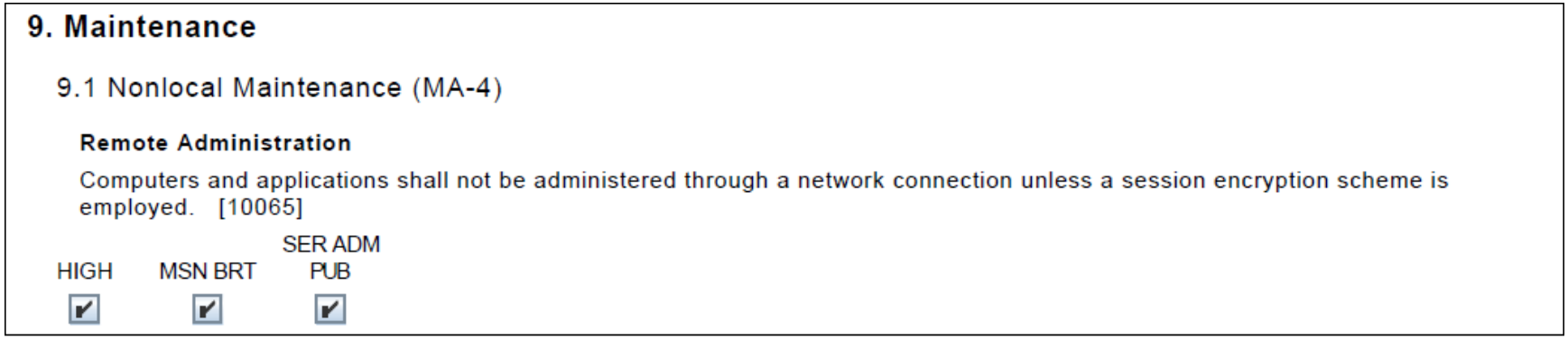

Figure 2: Requirement without Inventory Checkboxes

Consequences

The hardware, software, and data that support Information Technology activities at JPL belong to JPL, and therefore must be protected as specified in "JPL Cybersecurity Requirements," DocID 36852. Failure to do so puts all IT resources at risk, and can lead to loss of network privileges and disciplinary action, up to and including termination.

1. Access Control

1.1 Account Management (AC-2)

Root Account User ID

On Unix-based computers, only one account shall have a user id (uid) of 0. [11393]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☐	☑	☑	☑	☐

Account Owner Identification

User accounts on JPL IT assets shall only be provided to users whose identity is traceable to the corresponding identity in the JPL Directory.

Note: Data exchange between JPL IT assets is not precluded, but may not be used to allow access by unauthorized persons.

Note: This requirement does not apply to information cleared by Document Review for broad public dissemination. [11312]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

Account Review

The System Administrator shall review all information system accounts at least once every six months and delete unnecessary accounts. [11008]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

Account Deactivation

Individual user accounts shall be disabled or deleted if the password for the account has not been changed within 90 days after password expiration. [11216]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☐	☑	☑	☐	☐

1.2 Access Enforcement (AC-3)

Permitted Access

Access to information and IT assets shall be limited to authorized users, authorized processes acting on behalf of authorized users, and authorized devices.

Note: Access must be consistent with the restrictions described in "Marking and Handling Documentation" (JPL Rules! DocID 77806). [11088]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

Foreign Person Access Configuration

The System Administrator identified in an approved Computer Access Request (CAR) shall not permit a Foreign Person to use an IT asset on JPL's internal networks until it has been configured in accordance with the CAR, and the configuration has been verified by the JPL Cybersecurity/Identity Technologies & Operations Group.

Note: JPL's internal network IP address space is listed at https://net.jpl.nasa.gov/dns/ipspace.php. [11208]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

Foreign Person Access Restriction

Either the System Administrator identified in an approved Computer Access Request (CAR) or the JPL Research Network Administrator shall limit Foreign Person access to JPL's internal networks to the specific property numbers, IP addresses, and ports designated in the CAR.

Note: JPL's internal network IP address space is listed at https://net.jpl.nasa.gov/dns/ipspace.php. [11206]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☐	☑	☑	☑	☐

Access Control Review

The System Administrator shall review all access controls at least once every six months and modify them as necessary. [11348]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

1.3 Information Flow Enforcement (AC-4)

IP Filtering

Any IT asset providing IP services (e.g., sftp or ssh) shall employ IP filtering, when this capability is available. [11173]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☑	☑	☑	☑	☐

Limited External Release

JPL scientific or technical sites that are accessible outside the JPL network, but which restrict access, shall meet the requirements for limited external release of information, per "Release of Scientific or Technical Information" (JPL Rules! DocID 56614). [11349]

HIGH	MSN BRT	SER ADM PUB	Application
☑	☑	☑	☑

1.4 Separation of Duties (AC-5)

Independent Auditors

System administration/support personnel shall not function as independent auditors for their own IT System. [11205]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

1.5 Least Privilege (AC-6)

User Privileges

Users (or processes acting on behalf of users) shall be assigned the fewest privileges consistent with their assigned duties and functions. [11319]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☑	☑	☐	☐	☑	☐	☑	☑	☑	☐

User Privileges

In order to limit exposure, a user having access to multiple roles or accounts shall use the one with the least set of privileges to perform a given activity. [11460]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

Personnel with Administrative Privileges

Line managers, project managers, or their appointees shall identify the individuals having administrative privileges to computers and applications deployed on JPL's internal networks by updating the associated Information and Technology Solutions (ITSD) Directory Services authorization group.

Note: Users of general-purpose desktop computers administered under the Institutional Computing Environment (ICE) contract need not be identified.

Note: JPL's internal network IP address space is listed at https://net.jpl.nasa.gov/dns/ipspace.php. [11433]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☐	☑	☑	☐	☐	☐	☐	☑	☑	☑	☐

1.6 Unsuccessful Logon Attempts (AC-7)

Temporary Lockout

After 10 unsuccessful logon attempts within 15 minutes, IT assets and applications shall delay processing further logon attempts for 15 minutes when this capability cannot be achieved through the JPL Directory and Authentication Service (https://dir.jpl.nasa.gov/). [11086]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☑	☑	☐	☐	☐	☑	☑	☑	☐	☐

Temporary Lockout

After 10 unsuccessful logon attempts within 15 minutes, isolated IT assets and applications shall delay processing further logon attempts for 15 minutes unless this capability is either unavailable or incompatible with the intended use. [11452]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☑	☑	☐	☐	☐	☑	☑	☑	☐	☑

1.7 System Use Notification (AC-8)

Warning Banner

The following warning banner shall be displayed to the user, when feasible prior to granting access to a computer, otherwise immediately after an authenticated access is granted: "This computer is funded by the United States Government and operated by the California Institute of Technology in support of ongoing U.S. Government programs and activities. If you are not authorized to access this system, disconnect now. Users of this system have no expectation of privacy. By continuing, you consent to your keystrokes and data content being monitored." [10021]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☑	☑	☐	☐	☐

1.8 Session Lock (AC-11)

No User Input Activity

If there has been no user input activity for a fixed period of time, not to exceed 15 minutes, computer systems shall automatically suspend console access, when this capability is provided by the operating system.

Note: Real-time operations consoles that must remain continuously running are exempt from this requirement; on public access systems, this requirement applies to user input activity related to non-public access. [10097]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐

1.9 Session Termination (AC-12)

Session Inactivity

An application with an open, authenticated user session shall automatically terminate the session after 60 minutes of inactivity, where inactivity is defined as no data flowing between the client and the server. [11376]

HIGH	MSN BRT	SER ADM PUB	Application
☑	☑	☐	☑

1.10 Permitted Actions without Identification or Authentication (AC-14)

Anonymous FTP

Directories accessed through anonymous FTP shall be configured such that those permitting write access do not allow read or list access. [11177]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☐	☑	☑	☐	☐

1.11 Remote Access (AC-17)

Prior Authorization

Remote access to JPL's internal networks shall be restricted to authorized users.

Note: JPL's internal network IP address space is listed at https://net.jpl.nasa.gov/dns/ipspace.php. [11176]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

1.12 Access Control for Portable and Mobile Devices (AC-19)

Travel to Designated Countries

Laptops, mobile devices, and smartphones shall not be taken to a NASA designated country, except as permitted by https://ieco.jpl.nasa.gov/guidance/jpl-electronic-device-requirements-travel-designated-countries/.

Note: Loaner devices that will be reimaged before connecting to JPL's internal networks can be ordered from https://jpl.service-now.com/sp?id=sc_cat_item&sys_id=fbff33a8dbfc93408152f4b40f961911.

Note: JPL's internal network IP address space is listed at https://net.jpl.nasa.gov/dns/ipspace.php. [11439]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☑	☑	☐	☐	☐	☐	☑	☐

Returning from Foreign Travel

Any traveler returning from foreign travel with a JPL- or contractor-provided laptop or other electronic device shall complete an antivirus scan on the device before connecting it to any network, when antivirus software is specified by the Information and Technology Solutions Directorate (ITSD). [11335]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

1.13 Publicly Accessible Content (AC-22)

Web and FTP Public Access

JPL web and ftp sites that allow unlimited (public) access from outside the JPL network shall be cleared by Document Review Services of the Documentation Services Group (scientific or technical sites) or the Institutional Communications Office (public engagement or educational outreach sites). [11322]

HIGH	MSN BRT	SER ADM PUB	Application
☑	☑	☑	☑

2. Awareness and Training

2.1 Security Awareness Training (AT-2)

Annual User Training

Each person shall take role-appropriate cybersecurity awareness training before being provided system access, and annually thereafter. [11306]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

3. Audit and Accountability

3.1 Audit Events (AU-2)

Logon/Logoff

Successful and failed logons/logoffs shall be recorded in system and application log files. [11010]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☑	☑	☐	☐	☐	☑	☑	☑	☑	☐

Shutdown/Restart

All shutdowns and restart events shall be recorded in the system log files, when this capability is automatically provided by the operating system. [11029]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☑	☑	☑	☑	☐

Password Change

An audit record of a password change containing user ID, date, and time shall be logged when supported by the operating system. [11076]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☐	☑	☑	☑	☐

3.2 Content of Audit Records (AU-3)

Privacy Information Transmission

Applications and servers transmitting privacy information shall generate audit records for each transmission event that establish what type of event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or modules associated with the event. [11411]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☐	☑	☑	☐	☐	☐	☐	☑	☑	☑	☐

JPL ITSD Logging System

All IT assets having an IP address shall be configured to log application and system messages to the JPL ITSD logging system.

All IT assets having an IP address shall be configured to log application and system messages to the JPL ITSD logging system.

Note: This can either be accomplished by using a properly configured client or by sending system messages to an ITSD-designated syslog server as discussed at http://jplsoc.jpl.nasa.gov/syslog. [11220]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐

3.3 Audit Review, Analysis, and Reporting (AU-6)

System and Application Log Files

The System Administrator or designee shall review system log files weekly for suspicious or unusual activity.

Note: Use of automated mechanisms such as the ITSD-provided Splunk service (http://jplsplunk.jpl.nasa.gov/) or analysis scripts that process syslog files can greatly reduce the resources needed to comply with this requirement.

Note: Application log files should also be periodically reviewed. [11018]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

Foreign Person Log Files

For non-isolated computers, at least once per week, the System Administrator or the JPL Research Network Administrator shall review the Foreign Person access control configuration for compliance with each associated approved Computer Access Request (CAR), and report each review via the method specified by the JPL Cybersecurity/Identity Technologies & Operations Group. [11386]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐

Foreign Person Log Files

For isolated computers, at least once per 90 days, the System Administrator shall review the Foreign Person access control configuration for compliance with each associated approved Computer Access Request (CAR), and report each review via the method specified by the JPL Cybersecurity/Identity Technologies & Operations Group. [11215]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☐	☐	☐	☐	☑

3.4 Time Stamps (AU-8)

Clock Synchronization

When supported by the operating system, each computer shall be configured to have its system clock synchronized with a reliable time service at least once each 24 hours.

Note: JPL Network Time Service is described at https://jplnet.jpl.nasa.gov/ntp/. [11375]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐

3.5 Non-repudiation (AU-10)

Root-level Access

To support auditing, access to accounts with root-level privileges shall only be obtained after users log into their own valid, individual, non-privileged user account followed by escalating privileges to a root-level account.

Note: This requirement does not apply to general-purpose desktop computers administered under the Institutional Computing Environment (ICE) contract. [11388]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☐	☑	☑	☑	☐

3.6 Audit Record Retention (AU-11)

System Log Files

System log files shall be retained for at least 90 days. [11019]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☐	☐	☐	☑	☐

Foreign Person Access Log Files

Logs of Foreign Person access to devices on JPL's internal networks shall be retained by the System Administrator or the JPL Research Network Administrator, on-line or as an archive, for a minimum of 90 days.

Note: JPL's internal network IP address space is listed at https://net.jpl.nasa.gov/dns/ipspace.php. [11211]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☑	☑	☑	☑	☐

3.7 Audit Generation (AU-12)

System Log Files

Security-related events (http://cybersecurity.jpl.nasa.gov/security_related_events.php), when recorded, shall be recorded in the system log files.

Note: Users can be notified about updates to the list of security-related events by joining the Cybersecurity Mailing List (http://cybersecurity.jpl.nasa.gov/subscribe_cybersec_mailinglist.php). [11151]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☑	☑	☐	☐	☐	☑	☑	☑	☑	☐

4. Security Assessment and Authorization

4.1 Security Assessments (CA-2)

Annual Review

All security controls for each IT System shall be assessed annually. [11329]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

Certification of Security Controls

All security controls for each IT System shall be certified before the initial accreditation and before every subsequent re-accreditation. [11330]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

4.2 Security Authorization (CA-6)

Authorizing Official

Each IT System shall be authorized by an Authorizing Official (AO) within three months of its identification in the IT Security Database (ITSDB), at least every three years thereafter, upon major change, or when a new AO is assigned.

Note: If the new AO is willing to accept the currently documented risk in the ITSDB, then only an updated Authorization to Operate letter is needed. [11331]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

5. Configuration Management

5.1 Configuration Management Policy and Procedures (CM-1)

Communication and Network Services

All data communications and network services for the JPL network (https://net.jpl.nasa.gov/dns/ipspace.php), including wired, wireless, wide area, perimeter security, DNS, DHCP and remote access, shall only be provided by the Information and Technology Solutions DIrectorate (ITSD). [11435]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

Production Services Subnets

The Information and Technology Solutions DIrectorate (ITSD) shall designate and manage the Production Services Subnets whose purpose is to provide institutional services.

Note: The Production Services Subnets list can be found at https://net.jpl.nasa.gov/dns/ipspace.php. [11379]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

5.2 Baseline Configuration (CM-2)

Subscribed Computers Core Software

The core software (https://jpl.service-now.com/sp?id=kb_article_view&sysparm_article=KB0010293) initially installed on a computer belonging to IT System 537 (DNS Subscribed IT Assets) shall not be deactivated, removed, or bypassed by the user.

Note: Users wanting to reimage a subscribed computer must first coordinate its transfer from IT System 537 to another authorized IT System. [11405]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☐	☐	☐	☑	☐

Manufacturer Security Protection

JPL-provided mobile devices shall not be jailbroken or rooted. [11412]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☐	☑	☑	☐	☐	☐	☐	☑	☐

5.3 Security Impact Analysis (CM-4)

JPL Directory Service Attributes

Attributes supplied by the JPL Directory Service (https://dir.jpl.nasa.gov/) shall not be altered if the effect would be to circumvent security controls. [11402]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

5.4 Configuration Settings (CM-6)

Computers with Multiple Operating Systems

For a computer configured with multiple operating systems, or emulating additional operating systems, each operating system on the computer shall comply with cybersecurity requirements based on the highest information category of data accessible to any one operating system. [10090]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☐	☐	☐	☑	☐

JPL Standard Security Controls

Computers, smartphones, and mobile devices receiving JPL e-mail or storing JPL data shall be configured in accordance with JPL standard security controls.

Note: This requirement, which applies to personally-owned smartphones and mobile devices receiving JPL email or storing JPL data, may be enforced by ITSD-provided agents or other downloads that automatically maintain standard configuration settings. [11373]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☑	☑	☐	☐	☐	☐	☑	☐

Virtual Machine IP Address

A virtual machine with a routable IP address shall only use a static IP address. [11344]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐

DNS Server Selection

Devices connected to the JPL network (https://net.jpl.nasa.gov/dns/ipspace.php) shall be configured to only use ITSD-approved Domain Name System (DNS) servers for translating host names into IP addresses.

Note: The list of approved DNS server IP addresses can be found at https://net.jpl.nasa.gov/dns/about.php. [11414]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☑	☑	☑	☑	☑	☑	☐	☐

5.5 Least Functionality (CM-7)

Essential Capabilities Configuration

IT assets shall be configured to provide only essential capabilities. [11387]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☑	☐

Essential Capabilities Configuration

IT assets shall be configured to prevent the use of prohibited services.

Note: The list of prohibited IT services can be found at http://cybersecurity.jpl.nasa.gov/prohibiteditservices.php. [11459]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☑	☐

5.6 Information System Component Inventory (CM-8)

ITSDB Device Registration

Every network-capable device shall be represented in the IT Security Database (ITSDB). [11401]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☑	☑	☑	☑	☑	☑	☑	☐

Permitted Network Access

Only IT resources registered in the ITSDB and approved by the ITSD shall be permitted to access JPL's internal networks.

Note: JPL's internal network IP address space is listed at https://net.jpl.nasa.gov/dns/ipspace.php. [11461]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

Virtual Machine Records in the ITSDB

Each virtual machine having a planned or actual life of at least 30 days shall be represented in the IT Security Database (ITSDB) using an ITSD-approved property ID prefix.

Note: The list of ITSD-approved property ID prefixes can be found by logging in at https://itsdb.jpl.nasa.gov/itsdb/intro.cfm and then going to https://itsdb.jpl.nasa.gov/itsdb/help/batch_mode_instruction.cfm. [11327]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

Virtual Machine Records in the ITSDB

When a virtual machine has been decommissioned, the ITSDB shall be updated accordingly. [11342]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

Assignment of Property to Security Plans

Line managers or their appointees shall assign incoming property (including virtual machines with routable IP addresses) to security plans, and implement required security controls within 30 days of receipt of the new equipment notification. [11301]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

ASR Record Creation

The developer of a custom application shall ensure that the application is listed in the JPL Application Security Registry (ASR).

Note: This requirement applies to custom applications and to customized third-party software such as commercial off-the-shelf (COTS), government off-the-shelf (GOTS), modified off-the-shelf (MOTS), open source, and reused.

Note: A detailed list of characteristics of custom applications and third-party software can be found at http://cybersecurity.jpl.nasa.gov/appsec_dev_procedures.php.

Note: The JPL ASR can be found by logging in at https://itsdb.jpl.nasa.gov/itsdb/intro.cfm and then clicking on "ASR." [11380]

HIGH	MSN BRT	SER ADM PUB	Application
☑	☑	☑	☑

Assignment of ASR Records to Security Plans

Within 30 days of receiving a new Application Security Registry (ASR) notification, line managers or their appointees shall assign the associated applications to security plans and implement required security controls. [11389]

HIGH	MSN BRT	SER ADM PUB	Application
☑	☑	☑	☑

SaaS requires Application Security Registry (ASR) record

Any use of multiuser Software as a Service (SaaS) that is procured by JPL shall be listed in the JPL Application Security Registry (ASR).

Note: Each security plan can only contain one ASR record for a given URL.

Note: The JPL ASR can be found by logging in at https://itsdb.jpl.nasa.gov/itsdb/intro.cfm and then clicking on "ASR." [11462]

HIGH	MSN BRT	SER ADM PUB	Application
☑	☑	☑	☑

5.7 Software Usage Restrictions (CM-10)

Inappropriate Use

Users shall not establish or make use of any network protocol or system that compromises cybersecurity, is explicitly prohibited by the JPL Cybersecurity/Identity Technologies & Operations Group, or results in the violation of local, state, or federal law. [11325]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

5.8 User-Installed Software (CM-11)

Installation Privileges for Users

Each IT System shall identify and enforce rules governing the installation of software by users. [11367]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

6. Contingency Planning

6.1 Contingency Plan (CP-2)

Critical Assets

The System Representative shall identify as a critical asset in the IT Security Database (ITSDB) each device or application that supports a Project or Infrastructure function that must continue during an emergency. [11438]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

6.2 Contingency Plan Testing (CP-4)

Annual Testing

Each IT System's Contingency Plan shall be tested at least annually. [11190]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

Recovery Procedures

When an IT System has time-critical restoration needs, recovery procedures shall be tested to verify compliance with the recovery time objectives and recovery point objectives. [11092]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

6.3 Alternate Storage Site (CP-6)

System Backup Storage

The Contingency Planning Coordinator shall employ an alternate storage site for system backup information that complies with "IT Systems and Electronic Records (Data) Backup" (JPL Rules! DocID 77823).

Note: Use of an ITSD-provided backup service satisfies this requirement. [11354]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☐

Geographical Separation

The Contingency Planning Coordinator shall identify an alternate storage site that is geographically separated from the primary storage site so as not to be susceptible to the same hazards.

Note: Use of an ITSD-provided backup service satisfies this requirement. [11355]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☐

Accessibility

The Contingency Planning Coordinator shall identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions.

Note: Use of an ITSD-provided backup service satisfies this requirement. [11356]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☐

Configuration

The Contingency Planning Coordinator shall ascertain that the alternate storage site is configured to facilitate timely and effective recovery operations.

Note: Use of an ITSD-provided backup service satisfies this requirement. [11358]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☐

6.4 Alternate Processing Site (CP-7)

Resumption of Critical Functions

The Contingency Planning Coordinator shall identify an alternate processing site and initiate necessary agreements to permit the resumption of information system operations for critical mission/business functions within the time specified by section III.6, "Outage Impacts and Allowable Outage Times" of its security plan, when the primary processing capabilities are unavailable. [11359]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☐

Geographical Separation

An alternate processing site identified by the Contingency Planning Coordinator shall be sufficiently geographically distant so as not to be susceptible to the same hazards. [11360]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☐

Accessibility

The Contingency Planning Coordinator shall identify potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outline explicit mitigation actions. [11361]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☐

Priority of Service

The Contingency Planning Coordinator, when arranging for an alternate processing site, shall ensure the agreements contain priority-of-service provisions in accordance with the IT system's availability requirements. [11363]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☐

Configuration

The Contingency Planning Coordinator shall fully configure the alternate processing site so that it is ready to be used as the operational site supporting a minimum required operational capability. [11364]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☐

6.5 Information System Backup (CP-9)

Backup Versions

Multiple generations of backups shall be retained as appropriate with the results of the system-specific risk analysis and contingency plan. [11093]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

Off-site Backups

At least one of the two most recent backups shall be sent to secured off-site storage for IT assets processing or storing MSN or High information. [11022]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☐

6.6 Information System Recovery and Reconstitution (CP-10)

Backups

Backups and original distribution media, when necessary to protect against loss or corruption, shall be maintained to ensure that operating system, configuration settings, software, and data can be restored to a usable state after a disruption or failure. [11305]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

7. Identification and Authentication

7.1 Identification and Authentication (Organizational Users) (IA-2)

Account Authentication

Account access shall be controlled by a User ID authenticated by a password or by two-factor authentication. [11082]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☑	☑	☑	☑	☑	☐

Application Authentication

Applications that limit access to authorized users shall be controlled by a User ID authenticated by a password or by two-factor authentication. [11385]

HIGH	MSN BRT	SER ADM PUB	Application
☑	☑	☑	☑

Use of JPL Directory and Authentication Service

To protect the confidentiality of password transmission, unprivileged access to computers on JPL's internal networks shall only be authenticated via the JPL Directory and Authentication Service (https://dir.jpl.nasa.gov/).

Note: JPL's internal network IP address space is listed at https://net.jpl.nasa.gov/dns/ipspace.php.

Note: This requirement does not apply to computers in a dedicated development or test environment. [11317]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☐	☑	☑	☐	☐

Use of JPL Directory and Authentication Service

When authentication is needed, applications hosted on JPL's internal networks shall use one of the authentication services or interfaces provided by the JPL Directory and Authentication Service (https://dir.jpl.nasa.gov/).

Note: JPL's internal network IP address space is listed at https://net.jpl.nasa.gov/dns/ipspace.php.

Note: This requirement does not apply to a publicly accessible web site that uses authentication to control access to its content and does not allow access to other non-public, JPL network resources.

Note: This requirement does not apply to applications in a dedicated development or test environment. [11377]

HIGH	MSN BRT	SER ADM PUB	Application
☑	☑	☑	☑

Uniqueness

Group accounts with shared passwords shall not be used.

Note: This requirement does not apply to group accounts essential for real-time mission operations, where the risk of using shared passwords is mitigated through controlled physical access, and a daily record is retained for one year of the time periods that individual users had access to the group accounts. [11198]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☐	☑	☑	☑	☐

Two-factor Authentication

Network access to privileged accounts shall only be provided via two-factor authentication.

Note: This requirement does not apply to computers at Disaster Recovery sites that do not offer two-factor authentication. [11409]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☑	☑	☐	☐	☐	☑	☑	☑	☐	☐

7.2 Device Identification and Authentication (IA-3)

JPL Windows Domain

All Windows-based computers residing on JPL's internal networks shall be members of the JPL Windows Domain.

Note: JPL's internal network IP address space is listed at https://net.jpl.nasa.gov/dns/ipspace.php. [11316]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☐	☑	☑	☐	☐

MAC Address Registration

Users shall register the wired or wireless MAC address of their network interface card with their JPL Username before connecting to JPL's internal network DHCP or wireless service.

Note: JPL's internal network IP address space is listed at https://net.jpl.nasa.gov/dns/ipspace.php. [11323]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☑	☐	☑	☑	☑	☐

7.3 Authenticator Management (IA-5)

Password Delivery

Passwords shall be delivered in a secure manner. [11074]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

Password Delivery

Passwords shall only be provided to authorized and verified recipients. [11077]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

Password Complexity

Passwords shall be constructed in accordance with the standard criteria that follow, when supported by the operating system:
Contain:
- At least 8 characters
- Characters from at least three of these four character sets:
1) Lower-case letters
2) Upper-case letters
3) Numbers
4) Special characters such as: % - _ + . ! $ (Caution: Avoid use of the following characters, which may conflict with Oracle applications and other tools: [, } : # @ / \ *)

Do Not Contain:
- A dictionary word, either by itself or with other characters appended or prefixed to it.
For example, do not use:
- A Username
- A vendor name
- Name or nickname for a product
- Contractor name
- Division name
- Section name
- Group name
- Organization name, Project/task/program name
- Sports or other well-known team or group name
- Your first or last name
- Personal information, such as family names, pet names, etc.
- A series of repetitive or keyboard patterns, e.g., 12345678, qwertyu [11060]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☑	☑	☑	☑	☑	☐

Password Encryption

The JPL password shall not be stored unencrypted on non-volatile media. [11311]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

Password Encryption

Passwords shall be encrypted when stored unless encryption of embedded passwords renders them unusable, in which case, access shall be restricted to authorized personnel only. [11073]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☑	☑	☐	☐	☑	☑	☑	☑	☑	☐

Private Key Encryption

Private cryptographic keys shall be encrypted when stored unless encryption renders them unusable, in which case, access shall be restricted to authorized personnel only. [11391]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☑	☑	☑	☑	☑	☑	☑	☐

Password Encryption

Passwords used to authenticate from a JPL IT asset to outside the JPL network shall be encrypted during transmission if the remote system processes or stores non-public JPL data. [11315]

HIGH	MSN BRT	SER ADM PUB	Application
☑	☑	☑	☑

Password Assignment

User account passwords, when assigned, shall be changed during first sign-on. [11080]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

Default Passwords

All vendor-supplied accounts on each IT asset and application shall be disabled or shall have their default passwords changed within 24 hours of power-on and before connecting to the network. [11081]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

Password Lifetime

Passwords shall have an established lifetime not to exceed 90 days. [10101]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☑	☑	☑	☐	☐

Password Reuse

Passwords shall not be reused before 180 days have elapsed. [11072]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☑	☑	☑	☐	☐

Password Reuse

A user account for system access shall have used a minimum of 24 passwords before a password can be reused. [11071]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☑	☑	☑	☐	☐

7.4 Authenticator Feedback (IA-6)

Password Display

Passwords, when entered, shall not be displayed in clear text on the monitor. [11075]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

8. Incident Response

8.1 Incident Reporting (IR-6)

Suspected Incidents

Any suspected or detected cybersecurity incident shall be reported to the JPL Security Operations Center, via the JPL IT Unified Service Desk (x4-HELP, (818) 354-4357). [11117]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

Foreign Person Incidents

The System Administrator shall immediately report anomalous Foreign Person user activities, or any deviation from the configuration specified in the approved Computer Access Request (CAR), to the JPL Security Operations Center, via the JPL IT Unified Service Desk (x4-HELP, (818) 354-4357) for example. [11213]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

9. Maintenance

9.1 Nonlocal Maintenance (MA-4)

Remote Administration

Computers and applications shall not be administered through a network connection unless a session encryption scheme is employed. [10065]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

9.2 Maintenance Personnel (MA-5)

Authorized Personnel

Only personnel designated by the System Administrator, System Representative, or Line Manager shall be authorized to perform local or remote maintenance on the information system. [11365]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

10. Media Protection

10.1 Media Marking (MP-3)

External Labels

External labels shall be affixed to removable media and information system output indicating the distribution limitations, handling caveats and applicable security markings (if any) of the information. [11382]

HIGH	MSN BRT	SER ADM PUB
☑	☐	☐

10.2 Media Transport (MP-5)

Removal from Controlled Areas

To ensure that data is protected by full disk encryption, laptops removed from controlled areas (e.g., JPL or contractor sites) shall be shut down when not being actively used.

Note: Putting a laptop into sleep mode does not satisfy this requirement, since its data remains decrypted.

Note: This requirement does not apply if full disk encryption is unavailable. [11440]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☐	☐	☐	☑	☐

Removal from Controlled Areas

Media shall be protected during transport outside of controlled areas and transported only by authorized personnel. [11383]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☐

Foreign Travel

No personally-owned electronic device storing JPL information shall be taken outside of the United States. [11372]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

10.3 Media Sanitization (MP-6)

Reuse

All user data shall be deleted before an IT asset is reallocated to another user not needing access to the data. [11398]

HIGH	MSN BRT	SER ADM PUB
☐	☐	☑

Reuse

All user data shall be securely deleted before an IT asset is reallocated to another user not needing access to the data. [11195]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☐

On-site Destruction

Storage media containing Privacy Information shall be destroyed on site when no longer needed or operable.

Note: NIST SP 800-88 (Guidelines for Media Sanitization) provides approved methods for destroying media. [11416]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☐	☐	☑	☐	☐	☐	☐	☑	☑	☑	☐

Unrecoverable Data

Data on storage media shall be rendered unrecoverable prior to the media, or the equipment in which it resides, being excessed, replenished, or sent for off-site maintenance, repair or replacement.

Note: Arrangements for the recovery of data from failed media, regardless of vendor, shall only be made by contacting the JPL IT Unified Service Desk (x4-HELP, (818) 354-4357). [10011]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

Unrecoverable Data

Data and software belonging to JPL that reside in the cloud, or at an alternate processing or storage site, shall be rendered unrecoverable prior to the associated storage being released. [11449]

HIGH	MSN BRT	SER ADM PUB	Application
☑	☑	☑	☑

11. Physical and Environmental Protection

11.1 Physical Access Authorizations (PE-2)

Authorized Personnel

The list of personnel authorized to access controlled areas containing IT assets storing or processing MSN or High information shall be maintained and approved annually by the proper authority. [11194]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☐

11.2 Physical Access Control (PE-3)

Unattended Portable IT Assets

During non-working hours, unattended portable IT assets shall be secured in a locked office or cabinet, or by a tie-down device. [11371]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☐	☑	☑	☑	☐

BRT Asset Protection

Unattended IT assets storing BRT information shall be secured in a locked office or cabinet, or by a tie-down device. [10002]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☐	☑	☐	☐	☑	☑	☑	☐	☐	☑	☑	☑	☐

MSN Asset Protection

IT assets storing or processing MSN information shall be located in a room whose entrance is physically or electronically controlled, and whose access is logged. [10003]

HIGH	MSN BRT	SER ADM PUB
☐	☑	☐

High Asset Protection

IT assets storing or processing High information shall be located in a locked area controlled by the Protective Services Division via their physical presence, video surveillance, or an alarm system. [11352]

HIGH	MSN BRT	SER ADM PUB
☑	☐	☐

11.3 Access Control for Output Devices (PE-5)

Shoulder Surfing

Restricted Access Information shall be protected against being displayed to unauthorized persons. [11384]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

11.4 Temperature and Humidity Controls (PE-14)

Media Storage

Media storage facilities shall be environmentally controlled. [11153]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

12. Planning

12.1 System Security Plan (PL-2)

Security Planning

Line managers or their appointees shall create security plans for organizational IT resources. [11300]

HIGH	MSN	BRT	SER ADM PUB
☑	☑	☑	

12.2 Rules of Behavior (PL-4)

Inappropriate Use

Computers storing, processing or transmitting information categorized as High, or residing on the Production Services or Mission Subnets, shall not be used for personal purposes.

Note: The list of Production Services and Mission Subnets can be found at http://jplnet.jpl.nasa.gov.

Note: Production Services and Mission Subnets are monitored for inappropriate use. [11381]

HIGH	MSN	BRT	SER ADM PUB
☑	☑	☑	

Cooperation with System Administrators

Users shall cooperate with system administrators to eliminate vulnerabilities in a timely manner. [11303]

HIGH	MSN	BRT	SER ADM PUB
☑	☑	☑	

Cooperation with Investigations

Users shall comply with security investigations, including audits of their computers. [11217]

HIGH	MSN	BRT	SER ADM PUB
☑	☑	☑	

Network Security Scanning

Users shall not hinder network security scanning. [11218]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

Hacking

Users shall not conduct hacking or other questionable activities (e.g., port scanning, phishing, spoofing, penetration testing) unless approved by, and coordinated with, the JPL Cybersecurity/Identity Technologies & Operations Group. [11406]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

Vulnerability Scanning

Local firewalls on JPL's internal networks shall be configured to allow network vulnerability scans by the JPL Cybersecurity/Identity Technologies & Operations Group.

Note: JPL Cybersecurity/Identity Technologies & Operations Group scans JPL's internal network (but not Mission networks) from the subnet, 137.78.237.0/24.

Note: JPL's internal network IP address space is listed at https://net.jpl.nasa.gov/dns/ipspace.php. [11404]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐

Unapproved Cloud Services

The use of cloud services that have not been approved by the ITSD shall be limited to the cases listed at http://cybersecurity.jpl.nasa.gov/directives.php.

Note: Information about acquiring approved cloud services can be found at https://cloudservices.jpl.nasa.gov/support/faq. [11419]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☑	☑	☑	☑	☐	☐	☑	☐	☑	☐

Export Control

No JPL employee or resident affiliate shall use an IT asset or application to share information with a Foreign Person without approval from the Import/Export Control Office (I/ECO). [11313]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

13. Personnel Security

13.1 Position Risk Designation (PS-2)

Foreign Person Access Review

No System Administrator or JPL Research Network Administrator assigned to review Foreign Person access control configurations shall be a Foreign Person. [11309]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

System Administrator

No System Administrator for an IT asset on JPL's internal networks shall be a Foreign Person unless permitted by an approved Technology Transfer Control Plan.

Note: JPL's internal network IP address space is listed at https://net.jpl.nasa.gov/dns/ipspace.php. [11451]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

13.2 Access Agreements (PS-6)

Non-Disclosure Agreement

Each individual requiring access to other people's Privacy Information (PI) shall review and sign the Caltech/JPL Confidentiality and Non-Disclosure Agreement (http://forms.jpl.nasa.gov/form/7408/download) before accessing PI, and annually thereafter if the need for access continues. [11420]

HIGH	MSN	SER ADM BRT	PUB
☑	☑	☑	☑

14. Risk Assessment

14.1 Vulnerability Scanning (RA-5)

Application Black-box Assessment

Network-aware applications shall be scanned for vulnerabilities before being deployed on JPL's internal networks.

Note: The JPL Cybersecurity/Identity Technologies & Operations Group offers a scanning service as described at http://cybersecurity.jpl.nasa.gov/appsec_services.php.

Note: JPL's internal network IP address space is listed at https://net.jpl.nasa.gov/dns/ipspace.php. [11333]

HIGH	MSN	SER ADM BRT	PUB	Application
☑	☑	☑	☑	☑

15. System and Services Acquisition

15.1 Security Engineering Principles (SA-8)

Application Security

Application developers shall comply with the JPL Cybersecurity Procedures for Application Developers available at http://cybersecurity.jpl.nasa.gov/appsec_dev_procedures.php. [11378]

HIGH	MSN BRT	SER ADM PUB	Application
☑	☑	☑	☑

15.2 External Information System Services (SA-9)

Use of Approved Cloud Services

Only ITSD-approved cloud service providers shall be used to store, process, or transmit JPL data that is High, MSN, BRT, or SER. [11396]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

15.3 Unsupported System Components (SA-22)

End-of-life Software

Operating systems, middleware, and applications shall not be used when support is no longer available from the developer, vendor, or manufacturer, except for systems that provide critical mission/business capability for which newer technologies are not available.

Note: Plans for mitigating the risk to critical assets should be coordinated with the JPL Cybersecurity/Identity Technologies & Operations Group and documented in the associated security plan. [11422]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☑	☑	☑	☑	☐	☑	☑	☑	☐	☐

16. System and Communications Protection

16.1 Boundary Protection (SC-7)

Use of ITSD Services for External Access

Access to IT assets on JPL's internal networks shall not be provided from outside except via Information and Technology Solutions DIrectorate (ITSD) services, when such services are available.

Note: JPL's internal network IP address space is listed at https://net.jpl.nasa.gov/dns/ipspace.php.

Note: BrowserRAS and Virtual Private Network (VPN) access can be requested from https://ras.jpl.nasa.gov.

Note: Secure Shell (SSH) access can be requested from https://remote-ssh.jpl.nasa.gov.

Note: Users and automated processes can securely transfer large files using the JPL File Transfer service described at http://lft.jpl.nasa.gov.

Note: When no ITSD-provided service is available, a Zone Access Request (ZAR) can be submitted at https://zar.jpl.nasa.gov. [11310]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

Bridged Network Connections

IT resources shall not be simultaneously connected to multiple networks except when a service request (http://jplit.jpl.nasa.gov/formsE/f_RC.setIF.asp) has been approved by the JPL Network Service. [11436]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

Subscribed Computers

General-purpose desktop computers administered under the Institutional Computing Environment (ICE) contract shall not offer network services. [11351]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

Local Firewalls

When a local firewall is provided by the operating system, it shall be configured to deny access to all but essential incoming connections. [11403]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☐	☐	☐	☑	☐

Automatic Email Forwarding

No email addressed to the jpl.nasa.gov domain or any sub-domain shall be automatically routed or forwarded to domains other than .gov, caltech.edu, or .mil. [11374]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

No Anonymous Public Access to AFS

Unauthenticated external access shall not be provided to JPL's Andrew File System (AFS) resources. [11368]

HIGH	MSN BRT	SER ADM PUB	Application
☑	☑	☑	☑

16.2 Transmission Confidentiality And Integrity (SC-8)

Encryption

BRT information shall be encrypted when electronically transmitted outside of JPL's internal networks.

Note: JPL's internal network IP address space is listed at https://net.jpl.nasa.gov/dns/ipspace.php. [11458]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☐	☑	☑	☐	☐	☐	☐	☐	☑	☐	☐

Encryption

Privacy information, as defined by http://rules.jpl.nasa.gov/cgi/glossary2.pl?sl=P, shall be encrypted when electronically transmitted. [11326]

HIGH	MSN BRT	SER ADM PUB	Application
☑	☑	☑	☑

16.3 Cryptographic Protection (SC-13)

Encryption Products

When encrypting stored information, an ITSD-provided encryption product shall be used if available. [11105]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

Compliance with FIPS PUB 140-2

Data encryption, when used, shall use a cryptographic module validated against FIPS PUB 140-2 (Security Requirements for Cryptographic Modules).

Note: The list of validated modules can be found at http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm.

Note: The operator of a cryptographic module is responsible for ensuring that the algorithms and key lengths are in compliance with the requirements of NIST SP 800-131A Rev. 1 (Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths) (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf). [11103]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☑	☑	☐	☐	☐	☑	☑	☑	☑	☐

16.4 Session Authenticity (SC-23)

SSL Certificates

Web servers that use Secure Sockets Layer (SSL) certificates for authentication and communication encryption shall use valid SSL certificates obtained as described at https://ssl.jpl.nasa.gov/. [11415]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☑	☐	☐

16.5 Protection of Information at Rest (SC-28)

Mobile Devices, Smartphones, and Laptops

Every JPL- or contractor-provided mobile device, smartphone, and laptop shall employ full disk encryption (FDE) as specified by, or approved by, the Information and Technology Solutions DIrectorate (ITSD). [11369]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☑	☑	☐	☐	☐	☐	☐	☐

Privacy Information

Privacy information, as defined by http://rules.jpl.nasa.gov/cgi/glossary2.pl?sl=P, shall be protected at rest by virtual disk encryption, volume encryption, or file/folder encryption. [11457]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☐	☐	☑	☑	☑	☐	☐	☑	☐	☑	☐

Privacy Information

Any isolated mobile device, smartphone, or laptop that stores privacy information shall employ full disk encryption (FDE) as specified by, or approved by, the Information and Technology Solutions DIrectorate (ITSD). [11454]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☐	☐	☑	☑	☑	☐	☐	☐	☐	☐	☑

17. System and Information Integrity

17.1 Flaw Remediation (SI-2)

Software Updates

Security-related software updates shall be applied to each IT asset monthly or per Mission-specific patch management lifecycle.

Note: Computers must be rebooted within 7 days of patch application when needed to complete patch installation. [11193]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☑	☑	☑	☑	☑	☑	☐	☐

Software Updates

Security-related software updates shall be applied to each application within 90 days of release. [11390]

HIGH	MSN BRT	SER ADM PUB	Application
☑	☑	☑	☑

Patch Management Software

Patch management software shall be installed on all computers and configured to report patch status, when the client software is provided by the Information and Technology Solutions DIrectorate (ITSD). [11203]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☐	☑	☑	☐	☐

SPL Tickets

A vulnerability documented in a Security Problem Log (SPL) ticket shall be resolved and the resolution documented and approved prior to the expiration date of the ticket. [11318]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

17.2 Malicious Code Protection (SI-3)

Antivirus Software Installation

Antivirus software specified by the Information and Technology Solutions DIrectorate (ITSD) shall be installed. [11133]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☑	☑	☐	☐	☑	☑	☐	☐

Antivirus Software Installation

Antivirus software specified by the Information and Technology Solutions DIrectorate (ITSD) shall be installed on isolated devices unless this installation cannot be performed or is incompatible with the intended use. [11453]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☑	☑	☐	☐	☑	☑	☐	☑

Antivirus Software Update

Installed antivirus software shall be kept current with the latest versions, settings, and definition files supplied by the Information and Technology Solutions DIrectorate (ITSD). [11199]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☑	☑	☐	☐	☑	☑	☑	☐

Antivirus Software Scanning

Antivirus software specified by the Information and Technology Solutions DIrectorate (ITSD) shall be used to conduct full disk scans at least monthly. [11394]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☑	☑	☐	☐	☐	☑	☐	☐

17.3 Software, Firmware, and Information Integrity (SI-7)

File Integrity Monitoring

File integrity monitoring software approved by the Information and Technology Solutions DIrectorate (ITSD) shall be installed and configured to monitor changes to critical system files on MSN, High, and all externally accessible computers. [11219]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐

File Integrity Monitoring

The assigned System Administrator listed in an approved Computer Access Request (CAR) shall install file integrity monitoring software on all "keyboard" assets, when this software is institutionally provided, and configured to monitor changes to system-related files. [11336]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☐	☑	☐	☐	☐	☐	☐	☐	☑	☐

17.4 Information Input Validation (SI-10)

Prescreening Input

Custom web applications shall enforce validation in all input fields.

Note: http://cybersecurity.jpl.nasa.gov/appsec_dev_procedures.php provides additional guidance. [11434]

HIGH	MSN BRT	SER ADM PUB	Application
☑	☑	☑	☑

17.5 Information Handling and Retention (SI-12)

Restricted Access Information

Output containing restricted access information shall only be distributed to authorized personnel. [11129]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

18. Accountability, Audit, and Risk Management

18.1 Privacy Requirements for Contractors and Service Providers (AR-3)

Cloud Storage

JPL Privacy Information (PI) shall not be shared with a Software as a Service (SaaS) or cloud service provider until the provider's proposed measures for protecting JPL PI have been approved by the JPL Chief Information Security Officer or designee.

Note: Additional information can be found at http://cybersecurity.jpl.nasa.gov/directives.php. [11423]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☐	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐

18.2 Privacy Monitoring and Auditing (AR-4)

Need to Know

The justification for each user's access to Privacy Information (PI) shall be reviewed annually and approved by the PI owner and the user's line manager. [11424]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐

Directory Group Membership

If group membership in the JPL Directory and Authentication Service (https://dir.jpl.nasa.gov/groups/) is relied upon to enable access to privacy information as defined by http://rules.jpl.nasa.gov/cgi/glossary2.pl?sl=P, then this membership shall be annually reviewed by the group owner or administrator, and approved by the privacy information owner. [11426]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

Data Loss Prevention

Data Loss Prevention (DLP) software specified by the Information and Technology Solutions DIrectorate (ITSD) shall be installed on computers that store or process Privacy Information (PI) (as defined in http://rules.jpl.nasa.gov/cgi/glossary2.pl?sl=P). [11425]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☐	☐	☑	☐	☐	☐	☐	☐	☐	☐	☐

18.3 Privacy Awareness and Training (AR-5)

Annual Privacy Training

All individuals requiring access to other people's Privacy Information (PI) shall complete the PI training program (https://learning.jpl.nasa.gov) before accessing PI, and annually thereafter if PI access continues. [11427]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐

19. Data Minimization and Retention

19.1 Minimization of Personally Identifiable Information (DM-1)

Exposure of Privacy Information

When feasible, Privacy Information (PI) shall be removed, redacted, or anonymized. [11428]

HIGH	MSN BRT	SER ADM PUB	Application	CPU	Mobile Device	Smartphone	Network Printer	Network Component	Network Storage	LFND	Also Isolated	Only Isolated
☑	☑	☐	☑	☑	☐	☐	☐	☐	☑	☑	☑	☐

20. Use Limitation

20.1 Information Sharing with Third Parties (UL-2)

Prior Authorization

Privacy information shall not be shared unless approved by the Information and Technology Solutions DIrectorate. [11432]

HIGH	MSN BRT	SER ADM PUB
☑	☑	☑

Paper copies of this document may not be current and should not be relied on for official purposes. The current version is in the JPL Rules! Information System at http://rules.jpl.nasa.gov/.

Appendix A

Application Security Requirements

This appendix lists the subset of requirements for application developers.

1. Access Control

1.3 Information Flow Enforcement (AC-4)

Limited External Release

JPL scientific or technical sites that are accessible outside the JPL network, but which restrict access, shall meet the requirements for limited external release of information, per "Release of Scientific or Technical Information" (JPL Rules! DocID 56614). [11349]

1.5 Least Privilege (AC-6)

User Privileges

Users (or processes acting on behalf of users) shall be assigned the fewest privileges consistent with their assigned duties and functions. [11319]

Personnel with Administrative Privileges

Line managers, project managers, or their appointees shall identify the individuals having administrative privileges to computers and applications deployed on JPL's internal networks by updating the associated ITSD Directory Services authorization group.

Note: Users of general-purpose desktop computers administered under the Institutional Computing Environment (ICE) contract need not be identified.

Note: JPL's internal network IP address space is listed at https://net.jpl.nasa.gov/dns/ipspace.php. [11433]

1.6 Unsuccessful Logon Attempts (AC-7)

Temporary Lockout

After 10 unsuccessful logon attempts within 15 minutes, IT assets and applications shall delay processing further logon attempts for 15 minutes when this capability cannot be achieved through the JPL Directory and Authentication Service (https://dir.jpl.nasa.gov/). [11086]

Temporary Lockout

After 10 unsuccessful logon attempts within 15 minutes, isolated IT assets and applications shall delay processing further logon attempts for 15 minutes unless this capability is either unavailable or incompatible with the intended use. [11452]

1.9 Session Termination (AC-12)

Session Inactivity

An application with an open, authenticated user session shall automatically terminate the session after 60 minutes of inactivity, where inactivity is defined as no data flowing between the client and the server. [11376]

1.13 Publicly Accessible Content (AC-22)

Web and FTP Public Access

JPL web and ftp sites that allow unlimited (public) access from outside the JPL network shall be cleared by Document Review Services of the Documentation Services Group (scientific or technical sites) or the Institutional Communications Office (public engagement or educational outreach sites). [11322]

3. Audit and Accountability

3.1 Audit Events (AU-2)

Logon/Logoff

Successful and failed logons/logoffs shall be recorded in system and application log files. [11010]

3.2 Content of Audit Records (AU-3)

Privacy Information Transmission

Applications and servers transmitting privacy information shall generate audit records for each transmission event that establish what type of event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or modules associated with the event. [11411]

JPL ITSD Logging System

All IT assets having an IP address shall be configured to log application and system messages to the JPL ITSD logging system.

Note: This can either be accomplished by using a properly configured client or by sending system messages to an ITSD-designated syslog server as discussed at http://jplsoc.jpl.nasa.gov/syslog. [11220]

3.7 Audit Generation (AU-12)

System Log Files

Security-related events (http://cybersecurity.jpl.nasa.gov/security_related_events.php), when recorded, shall be recorded in the system log files.

Note: Users can be notified about updates to the list of security-related events by joining the Cybersecurity Mailing List (http://cybersecurity.jpl.nasa.gov/subscribe_cybersec_mailinglist.php). [11151]

5. Configuration Management

5.5 Least Functionality (CM-7)

Essential Capabilities Configuration

IT assets shall be configured to provide only essential capabilities. [11387]

Essential Capabilities Configuration

IT assets shall be configured to prevent the use of prohibited services.

Note: The list of prohibited IT services can be found at http://cybersecurity.jpl.nasa.gov/prohibiteditservices.php. [11459]

5.6 Information System Component Inventory (CM-8)

ASR Record Creation

The developer of a custom application shall ensure that the application is listed in the JPL Application Security Registry (ASR).

Note: This requirement applies to custom applications and to customized third-party software such as commercial off-the-shelf (COTS), government off-the-shelf (GOTS), modified off-the-shelf (MOTS), open source, and reused.

Note: A detailed list of characteristics of custom applications and third-party software can be found at http://cybersecurity.jpl.nasa.gov/appsec_dev_procedures.php.

Note: The JPL ASR can be found by logging in at https://itsdb.jpl.nasa.gov/itsdb/intro.cfm and then clicking on "ASR." [11380]

Assignment of ASR Records to Security Plans

Within 30 days of receiving a new Application Security Registry (ASR) notification, line managers or their appointees shall assign the associated applications to security plans and implement required security controls. [11389]

7. Identification and Authentication

7.1 Identification and Authentication (Organizational Users) (IA-2)

Application Authentication

Applications that limit access to authorized users shall be controlled by a User ID authenticated by a password or by two-factor authentication. [11385]

Use of JPL Directory and Authentication Service

When authentication is needed, applications hosted on JPL's internal networks shall use one of the authentication services or interfaces provided by the JPL Directory and Authentication Service (https://dir.jpl.nasa.gov/).

Note: JPL's internal network IP address space is listed at https://net.jpl.nasa.gov/dns/ipspace.php.

Note: This requirement does not apply to a publicly accessible web site that uses authentication to control access to its content and does not allow access to other non-public, JPL network resources.

Note: This requirement does not apply to applications in a dedicated development or test environment. [11377]

Two-factor Authentication

Network access to privileged accounts shall only be provided via two-factor authentication.

Note: This requirement does not apply to computers at Disaster Recovery sites that do not offer two-factor authentication. [11409]

7.3 Authenticator Management (IA-5)

Password Encryption

Passwords shall be encrypted when stored unless encryption of embedded passwords renders them unusable, in which case, access shall be restricted to authorized personnel only. [11073]

Password Encryption

Passwords used to authenticate from a JPL IT asset to outside the JPL network shall be encrypted during transmission if the remote system processes or stores non-public JPL data. [11315]

10. Media Protection

10.3 Media Sanitization (MP-6)

Unrecoverable Data

Data and software belonging to JPL that reside in the cloud, or at an alternate processing or storage site, shall be rendered unrecoverable prior to the associated storage being released. [11449]

12. Planning

12.2 Rules of Behavior (PL-4)

Unapproved Cloud Services

The use of cloud services that have not been approved by the ITSD shall be limited to the cases listed at http://cybersecurity.jpl.nasa.gov/directives.php.

Note: Information about acquiring approved cloud services can be found at https://cloudservices.jpl.nasa.gov/support/faq. [11419]

14. Risk Assessment

14.1 Vulnerability Scanning (RA-5)

Application Black-box Assessment

Network-aware applications shall be scanned for vulnerabilities before being deployed on JPL's internal networks.

Note: The JPL Cybersecurity/Identity Technologies & Operations Group offers a scanning service as described at http://cybersecurity.jpl.nasa.gov/appsec_services.php.

Note: JPL's internal network IP address space is listed at https://net.jpl.nasa.gov/dns/ipspace.php. [11333]

15. System and Services Acquisition

15.1 Security Engineering Principles (SA-8)

Application Security

Application developers shall comply with the JPL Cybersecurity Procedures for Application Developers available at http://cybersecurity.jpl.nasa.gov/appsec_dev_procedures.php. [11378]

15.3 Unsupported System Components (SA-22)

End-of-life Software

Operating systems, middleware, and applications shall not be used when support is no longer available from the developer, vendor, or manufacturer, except for systems that provide critical mission/business capability for which newer technologies are not available.

Note: Plans for mitigating the risk to critical assets should be coordinated with the JPL Cybersecurity/Identity Technologies &

Operations Group and documented in the associated security plan. [11422]

16. System and Communications Protection

16.1 Boundary Protection (SC-7)

No Anonymous Public Access to AFS

Unauthenticated external access shall not be provided to JPL's Andrew File System (AFS) resources. [11368]

16.2 Transmission Confidentiality And Integrity (SC-8)

Encryption

BRT information shall be encrypted when electronically transmitted outside of JPL's internal networks.

Note: JPL's internal network IP address space is listed at https://net.jpl.nasa.gov/dns/ipspace.php. [11458]

16.3 Cryptographic Protection (SC-13)

Compliance with FIPS PUB 140-2

Data encryption, when used, shall use a cryptographic module validated against FIPS PUB 140-2 (Security Requirements for Cryptographic Modules).

Note: The list of validated modules can be found at http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm.

Note: The operator of a cryptographic module is responsible for ensuring that the algorithms and key lengths are in compliance with the requirements of NIST SP 800-131A Rev. 1 (Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths) (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar1.pdf). [11103]

16.4 Session Authenticity (SC-23)

SSL Certificates

Web servers that use Secure Sockets Layer (SSL) certificates for authentication and communication encryption shall use valid SSL certificates obtained as described at https://ssl.jpl.nasa.gov/. [11415]

17. System and Information Integrity

17.1 Flaw Remediation (SI-2)

Software Updates

Security-related software updates shall be applied to each application within 90 days of release. [11390]

17.4 Information Input Validation (SI-10)

Prescreening Input

Custom web applications shall enforce validation in all input fields.

Note: http://cybersecurity.jpl.nasa.gov/appsec_dev_procedures.php provides additional guidance. [11434]

18. Accountability, Audit, and Risk Management

18.1 Privacy Requirements for Contractors and Service Providers (AR-3)

Cloud Storage

JPL Privacy Information (PI) shall not be shared with a Software as a Service (SaaS) or cloud service provider until the provider's proposed measures for protecting JPL PI have been approved by the JPL Chief Information Security Officer or designee.

Note: Additional information can be found at http://cybersecurity.jpl.nasa.gov/directives.php. [11423]

18.2 Privacy Monitoring and Auditing (AR-4)

Need to Know

The justification for each user's access to Privacy Information (PI) shall be reviewed annually and approved by the PI owner and the user's line manager. [11424]

18.3 Privacy Awareness and Training (AR-5)

Annual Privacy Training

All individuals requiring access to other people's Privacy Information (PI) shall complete the PI training program (https://learning.jpl.nasa.gov) before accessing PI, and annually thereafter if PI access continues. [11427]

19. Data Minimization and Retention

19.1 Minimization of Personally Identifiable Information (DM-1)

Exposure of Privacy Information

When feasible, Privacy Information (PI) shall be removed, redacted, or anonymized. [11428]

Appendix B – Glossary

GLOSSARY

Glossary Notes

1. CNSS refers to the Committee on National Security Systems glossary.
2. NIST Special Publication (SP) documents can be found at http://csrc.nist.gov/publications/PubsSPs.html

Term	Definition
Access	Ability to make use of any information system (IS) resource. (NIST SP 800-32)
ADM	Administrative Information Category
Audit	Independent review and examination of records and activities to assess the adequacy of system controls and ensure compliance with established policies and operational procedures. (CNSS)
Audit log	A chronological record of system activities. Includes records of system accesses and operations performed in a given period. (CNSS)
Audit record	An individual entry in an audit log related to an audited event. (NIST 800-53 Rev. 4)
Authenticate	To confirm the identity of an entity when that identity is presented. (NIST SP 800-32)
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system. (FIPS PUB 200)
Authorization to operate (ATO)	The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls. (NIST SP 800-53 Rev 4)

Term	Definition
Authorized user	Any appropriately cleared individual with a requirement to access an information system (IS) for performing or assisting in a lawful JPL purpose. (DoD 8570.01 (adapted))
Authorizing official	A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. (NIST SP 800-53 Rev 4)
BRT	Business and Restricted Technology Information Category
Certificate	A digital representation of information which at least (1) identifies the certification authority (CA) issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. (NIST SP 800-32)
Cloud computing	A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. (NIST SP 800-145)
Confidentiality	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. (44 U. S. Code Sec 3542)
File/folder encryption	The process of encrypting individual files or folders on a storage medium and permitting access to the encrypted data only after proper authentication is provided. (NIST SP 800-111)
Full disk encryption (FDE)	The process of encrypting all the data on the hard drive used to boot a computer, including the computer's OS, and permitting access to the data only after successful authentication to the FDE product. Also known as whole disk encryption. (NIST SP 800-111)
Integrity	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. (44 U.S.C. Sec. 3542)
MSN	Mission Information Category

Term	Definition
Network-aware	Accessible from one of JPL's internal networks listed at https://net.jpl.nasa.gov/dns/ipspace.php.
Privilege	A right granted to an individual, a program, or a process. (CNSS)
Privileged account	An information system account with authorizations of a privileged user. (NIST 800-53 Rev. 4)
Privileged user	A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. (CNSS)
PUB	Public Access Information Category
SaaS	Software as a Service.
SER	Scientific, Engineering, and Research Information Category
Virtual disk encryption	The process of encrypting a file called a container, which can hold many files and folders, and permitting access to the data within the container only after proper authentication is provided, at which point the container is typically mounted as a virtual disk. (NIST SP 800-111)
Volume encryption	The process of encrypting an entire logical volume and permitting access to the data on the volume only after proper authentication is provided. Volume encryption of boot and system volumes is essentially a special form of FDE. (NIST SP 800-111)