



NASA TECHNICAL HANDBOOK

National Aeronautics and Space Administration

ITS-HBK-2810.03-02 v2024-02

Published: 2024-02-23

**Planning
TECHNICAL HANDBOOK**

TABLE OF CONTENTS

Document Properties	3
Document History Log	3
Approval	3
1. Introduction	4
1.1. Purpose	4
1.2. Scope	4
1.3. Point of Contact(s)	4
1.4. Applicability	5
1.5. Applicable Documents	5
1.5.1. Federal Information Processing Standards (FIPS)	5
1.5.2. National Institute of Standards and Technology (NIST)	5
1.5.3. National Aeronautics and Space Administration (NASA)	5
1.5.4. Cancellations or Updates	5
2. Security Controls	5
2.1. System Security and Privacy Plan (SSP) (PL-2)	5
2.1.1. Information System Owner (ISO)	5
2.2. System Security Plan Plan/Coordinate with Other Organizational Entities (PL-2(3))	6
2.2.1. Information System Owner (ISO)	6
2.3. Rules of Behavior (PL-4)	6
2.3.1. Information System Owner (ISO)	7
2.3.2. Information Technology Security Awareness and Training Coordinator (ITSATC)	7
2.4. Rules of Behavior Social Media and Networking Restrictions (PL-4(1))	7
2.4.1. Senior Agency Information Security Officer (SAISO)	7
2.5. Security and Privacy Architecture (PL-8)	7
2.5.1. Information System Owner (ISO)	7
Appendix A: Acronyms	7

DOCUMENT PROPERTIES

Document History Log

Document Version	Published Date	Description
1.0	2011-05-02	Initial Document.
1.1	2013-04-30	Extended for 1 year.
1.2	2014-04-24	Extended while revision 4 updates are rolled into the handbook.
1.3	2014-12-08	One-year extension for revision and updates.
1.4	2015-03-09	Updated TOC and Rev 4 controls (PL-5, PL-8).
1.5	2018-01-12	Revised into new Handbook format.
1.6	2018-08-15	Revised into new Handbook format.
1.7	2019-10-01	Annual Review completed; minor administrative updates to handbook.
1.8	2021-09-30	Updated with NIST SP 800-53 Rev. 5 provisions.
1.9	2023-01-31	Annual update.
v2023-06	2023-06-16	Updated to new format
v2024-02	2024-02-23	Annual update

Approval

Approved:

Associate Chief Information Officer for
Cybersecurity & Privacy

1. INTRODUCTION

NASA requirements for protecting the security of NASA information and information systems are derived from National Institute of Standards and Technology (NIST) guidance. Information System Owners (ISOs) and other personnel responsible for the protection of NASA information or information systems shall follow NIST guidance in the proper security categorization ([FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*](#)), and in the selection and implementation of information security controls ([FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*](#) and [NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*](#)), in a manner consistent with the Risk Management Framework ([NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*](#)). NASA Policy Directive (NPD) 2810.1, NASA Information Security Policy, NASA Procedural Requirements (NPR) 2810.1, Security of Information and Information Systems, and the collection of 2810 Information Technology Handbooks (ITS-HBK) satisfy the policy and procedure controls of NIST SP 800-53 Rev. 5.

[NPR 2810.1](#) designates this handbook as a guide of NASA's Planning (PL) information security controls. The content of this document, in conjunction with NPD/R 2810.1, defines NASA policy and procedures to address [PL-1](#). This handbook supports implementation of requirements in [NPR 2810.1](#) and [NPD 2810.1](#). The Agency's Organization-Defined Values (ODVs) integrated into the control requirements within RSA ARCHER in the Risk Information Security Compliance System (RISCS) system.

The Planning control family relates to the definition and documentation of the key resources and activities used to protect Agency information and information systems. Effective security planning is both comprehensive and flexible. NASA uses a System Security Plan (SSP) template that specifies the set of information controls that must be considered for each system. The plan content for any specific system is governed by a risk assessment of the particular threats facing the system and a tailoring of security controls to meet those threats.

1.1. Purpose

This Handbook augments NIST guidance by providing NASA-specific requirements, procedures and recommendations, where applicable. NASA-specific guidance does not negate NIST guidance, unless explicitly stated.

In conjunction with NPD/R 2810.1 and NPD/R 1382, the content of this document defines NASA Policy and Procedures to address the [PL-2](#), [PL-4](#), [PL-8](#) control family.

1.2. Scope

This Handbook applies to all information system security planning activities conducted at NASA.

Although NASA handbooks may contain "shall" (requirements) statements, they are not intended to be requirements documents. Portions of NASA handbooks containing procedural or process guidance may be cited in contract, program, and other Agency documents, such as a NASA Policy Directive or NASA Procedural Requirement.

This Handbook and the policy/procedural guidance contained within remains in full force and effect until such time that the Handbook is formally cancelled, rescinded, or superseded by an updated document.

A documented rationale and/or justification shall accompany any non-concurrence, disapproval, denial, or request for deviation from the policy guidance or procedural requirements set forth in this Handbook to support such decision. The documented rationale/justification shall be provided to the NASA Cybersecurity and Privacy Division (CSPD) and the point of contact for this Handbook, in coordination with Center Chief Information Security Officers (CISO), to review and validate for the record.

1.3. Point of Contact(s)

For any questions or comments regarding the contents of this Handbook, contact:

- hq-dl-cspdpolicy@mail.nasa.gov

Any questions or concerns regarding perceived gaps in policy or implementation guidance, conflicting procedural requirements, lack of clarity pertaining to specified roles and responsibilities, or issues associated with interpretation shall be elevated to the NASA CSPD, in coordination with the CISO, and directed to the attention of the point of contact for this particular Handbook to address and resolve.

1.4. Applicability

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

1.5. Applicable Documents

1.5.1. Federal Information Processing Standards (FIPS)

- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*

1.5.2. National Institute of Standards and Technology (NIST)

- NIST SP 800-30, *Guide for Conducting Risk Assessments*
- NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*

1.5.3. National Aeronautics and Space Administration (NASA)

- NPD 2810.1, *NASA Information Security Policy*
- NPR 1382.1, *NASA Privacy Procedural Requirements*
- NPR 2810.1, *Security of Information and Information Systems*
- NASA-SPEC-2661.ODVr5, *NASA's Organization-Defined Values for NIST SP 800-53 Revision 5*

1.5.4. Cancellations or Updates

- None

2. SECURITY CONTROLS

2.1. System Security and Privacy Plan (SSP) (PL-2)

2.1.1. Information System Owner (ISO)

The ISO:

- Shall ensure every information system is documented by a SSP in RISCs.
- Develops a security and privacy plan for the system that:
 - Is consistent with the organization's enterprise architecture;
 - Explicitly defines the constituent system component;
 - Describes the operational context of the system in terms of mission and business processes;
 - Describes any specific threats to the system that are of concern to the organization;
 - Provides the results of a privacy risk assessment for systems processing personally identifiable information;
 - Identifies any relevant control baselines or overlays, if applicable;
 - Describes the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;
 - Is reviewed and approved by the authorizing official or designated representative prior to implementation;
 - Includes risk determinations for security and privacy architecture and design decisions;
 - Includes security- and privacy-related activities affecting the system that require planning and coordination with individuals or groups defined by NASA ODVs.
- Communicates subsequent changes to SSPs.
- Review the plans at frequency defined by NASA's ODV at [NASA-SPEC-2661.ODVr5](#), [NASA's Organization-Defined Values for NIST SP 800-53 Revision 5](#).
- Update the plans to address changes to the system and environment of operation or problems identified during plan implementation or control assessments.
- Ensures all SSPs are reviewed and updated in accordance with NASA ODVs.
 - Changes that invalidate already documented controls, control implementations, or risk levels warrant updates to an information system's SSP.
- Ensures all SSPs:
 - Include sufficient information to enable an implementation that is unambiguously compliant with the intent of the plan and a subsequent determination of risk if the plan is implemented;
 - Explicitly define the authorization boundary for the system;
 - Include a description of the operational environment of the information system in terms of related missions and business processes;
 - Include the security categorization of the information system including supporting rationale; and
 - Provide an overview of the security requirements for the system.

2.2. System Security Plan | Plan/Coordinate with Other Organizational Entities (PL-2(3))

2.2.1. Information System Owner (ISO)

The ISO:

- Plans and coordinates security-related activities affecting the information system with the CISO before conducting such activities in order to reduce the impact on other organizational entities.

2.3. Rules of Behavior (PL-4)

- NASA's Cybersecurity and Privacy Rules of Behavior are managed by OCIO and agreed to by each NASA User annually

2.3.1. Information System Owner (ISO)

The ISO:

- Ensures the use of information systems is restricted to NASA-approved users, as defined by Agency access and identity management systems (e.g., NASA Access Management Systems (NAMS)).
- Establishes and implements rules of behavior specific to their system, if necessary, as part of the account management process.

2.3.2. Information Technology Security Awareness and Training Coordinator (ITSATC)

The Information Technology Security Awareness and Training Coordinator (ITSATC):

- The ITSATC manager — Ensures that NASA's annual Cybersecurity and Privacy Awareness Training Course is provided and available to NASA Users.

2.4. Rules of Behavior | Social Media and Networking Restrictions (PL-4(1))

2.4.1. Senior Agency Information Security Officer (SAISO)

The SAISO:

- Provides cybersecurity and privacy rules of behavior, that include
 - Use of social media, social networking sites, and external sites/applications;
 - Posting organizational information on public websites; and
 - Use of NASA-provided identifiers (e.g., email addresses) and authentication secrets (e.g., passwords) for creating accounts on external sites/applications.

2.5. Security and Privacy Architecture (PL-8)

2.5.1. Information System Owner (ISO)

The ISO:

- Coordinates with the Senior Agency Official for Privacy/Chief Privacy Officer to enable identification of sensitive privacy information (i.e., personally identifiable information) and effective implementation of controls that fulfill privacy requirements.

APPENDIX A: ACRONYMS

CISO [Center] Chief Information Security Officer

FFRDC Federally Funded Research and Development Center

FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
HBK	Handbook
ISO	Information System Owner
IT	Information Technology
ITS	Information Technology Security
ITSATC	Information Technology Security Awareness and Training Coordinator
ITSD	Information Technology Security Division
NAMS	NASA Account Management System
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
OCIO	Office of the Chief Information Officer
PL	Planning
PM	Project Manager
RISCS	Risk Information Security Compliance System
SOC	Security Operations Center
SAISO	Senior Agency Information Security Officer
SP	Special Publication
SR	Service Request
SSP	System Security Plan