



NASA TECHNICAL HANDBOOK

National Aeronautics and Space Administration

ITS-HBK-2810.13-01 v2024-02

Published: 2024-02-23

**Personnel Security
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 and Corresponding Roles and Responsibilities	5
2.1. Position Risk Designation (PS-2)	6
2.1.1. Information System Owner (ISO) and/or Supervisor	6
2.2. Personnel Screening (PS-3)	6
2.2.1. Information System Owner (ISO) and/or Supervisor	6
2.3. Personnel Termination (PS-4)	6
2.3.1. NASA Human Resources (HR) and/or Supervisor	6
2.3.2. Information System Owner (ISO) and/or Supervisor in Coordination with ISSO	6
2.3.3. Chief of Security or Their Designee	6
2.3.4. Information System Security Officer (ISSO)	7
2.4. Personnel Transfers(PS-5)	7
2.4.1. Supervisor	7
2.4.2. Information System Owner (ISO)	7
2.4.3. Center Chief of Security	7
2.5. Access Agreements (PS-6)	7
2.5.1. Information System Owner (ISO)	7
2.6. External Personnel Security (PS-7)	7
2.6.1. Center Chief Information Security Officer (Center CISO)	7
2.6.2. Information System Security Officer (ISSO)	7
2.6.3. Information System Owner (ISO)	8
2.7. Personnel Sanctions (PS-8)	8
2.7.1. Center Chief Information Security Officer (Center CISO)	8
2.7.2. Enterprise Services and Integration Division	8
Appendix A: Acronyms	8

DOCUMENT PROPERTIES

Document History Log

Document Version	Published Date	Description
1.0	2011-05-02	Initial Draft
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	2015-03-20	Revised for Rev 4 controls & TOC • (PS-2) Changed wording to Position Risk Designation
1.4	2017-04-15	Updated to reflect new tools and maintain consistency with referenced documents/standards
1.5	2018-08-08	Updated to new Handbook format
1.6	2018-10-01	Mandatory review step added as a pilot project.
1.7	2019-11-19	NODIS consistency review
1.8	2021-09-20	Update to reflect SP 800-53r5
1.9	2023-01-31	Annual update.
v2023-06	2023-06-16	Updated to new format
v2024-02	2024-02-23	Annual update

Approval



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 will follow NIST guidance in the proper security categorization (Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization for 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 Special Publication (SP) 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations, in a manner consistent with the Risk Management Framework (NIST SP 800-37 Revision 2, 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 tool of NASA's Personnel Security (PS) information security controls, and the content of this document, in conjunction with NPD/R 2810.1, defines NASA policy and procedures to address [PS-1](#).

This handbook follows the requirements in NPR 2810.1 and NPD 2810.1. It also augments NIST guidance with procedures and recommendations, where applicable. NASA-specific guidance does not negate NIST guidance, unless explicitly stated. The Agency's organizationally defined values are integrated into the control requirements within RSA ARCHER in the Risk Information Security Compliance System (RISCS).

1.1. Purpose

The Personnel Security control family relates to the IT and physical security activities that surround various facets of the employment life cycle (i.e., initial employee screening, position categorization, authority delegation, sanctioning, transfers, and termination). Personnel Security controls mitigate the risk of staff and contractors exploiting their access privileges to NASA's assets or premises for unauthorized purposes.

1.2. Scope

Personnel Security applies to both direct employees of the Agency and contracted personnel, as well as service providers operating systems on behalf of NASA.

Although NASA handbooks may contain "shall" (requirements) statements, they are not intended to be requirements documents. However, pursuant to [NPR 1400.1](#), portions of NASA handbooks containing procedural or process guidance may be cited in contract, program, and other Agency documents, and may become requirements when a NASA directive specifies their use by citing the document title, revision letter/number, and date; or, when a NASA manager with authority over a NASA program, project, or other activity, identifies it as a requirement.

This Handbook and the 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 will accompany any non-concurrence, disapproval, denial, or request for deviation from the procedural guidance set forth in this Handbook to support such a decision. The documented rationale/justification is 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 should be elevated to the NASA CSPD, in coordination with the Center 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 800-37, *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)

- NASA Federal Acquisitions Regulation (FAR) Supplement 1852-204-76
 - NPd 2810.1, *NASA Information Security Policy*
 - NPR 1441.1, *NASA Records Management Program Requirements*
 - NPR 1600.1, *NASA Security Program Procedural Requirements*
 - NPR 2810.1, *Security of Information and Information Systems*

1.5.4. Cancellations or Updates

- ITS-HBK-2810.13-01

2. SECURITY CONTROLS AND CORRESPONDING ROLES AND RESPONSIBILITIES

The following controls apply to information systems categorized as a Low or Moderate system with a Low or Moderate security control baseline (per NIST SP 800-53). Additional controls and NASA Organizationally Defined Values (ODV) will apply to systems that are categorized as a High system, but are not listed here.

2.1. Position Risk Designation (PS-2)

2.1.1. Information System Owner (ISO) and/or Supervisor

The ISO and/or Supervisor:

- Ensures that all access to a system or a system accreditation boundary is granted only to authorized individuals who hold position risk designations (e.g. from NASA Personnel Security, OPM, or other approved methods) that are commensurate with the sensitivity of the information system.
- Ensures the periodic review and revision of risk designation occurs for positions that may access their system, and ensure that those position risk designations remain commensurate with the sensitivity of the information system.

2.2. Personnel Screening (PS-3)

2.2.1. Information System Owner (ISO) and/or Supervisor

The ISO and/or Supervisor:

- Ensures that all access to a system or a system accreditation boundary is granted only to authorized individuals who hold position risk designations (e.g. from NASA Personnel Security, OPM, or other approved method) that are commensurate with the sensitivity of the information system.
 - Screening criteria includes establishing the suitability/eligibility for personnel having System Security Responsibilities (SSR) and the minimum requiring investigation based on the position categorization.

2.3. Personnel Termination (PS-4)

2.3.1. NASA Human Resources (HR) and/or Supervisor

The NASA Human Resources (HR) and/or Supervisor:

- Ensures completion of the “Employee Termination” request in the NASA Identity Management and Account Exchange (IdMAX) system.
 - Retrieves all security-related NASA information, property, and materials. Ensure proper storage of data after user is terminated in the event it is needed by the SOC, HR or CISO.
- Retains and ensures access to all NASA information and information systems formally controlled by the terminated individual.

2.3.2. Information System Owner (ISO) and/or Supervisor in Coordination with ISSO

The ISO and/or Supervisor in Coordination with ISSO:

- Ensures, upon termination of individual employment, termination of information system access that is not managed through the IdMAX system.

2.3.3. Chief of Security or Their Designee

The Chief of Security or Their Designee

- Ensures that personnel are properly debriefed prior to termination.

2.3.4. Information System Security Officer (ISSO)

The ISSO:

- Ensures that all security-related organizational system-related property is retrieved.

2.4. Personnel Transfers(PS-5)

2.4.1. Supervisor

The Supervisor:

- Manages the return of and issuing of new keys, building passes, etc.
- Provides access to official records that the employee had access to at previous work locations or on prior accounts, as appropriate and in accordance with NPR 1441.1E.

2.4.2. Information System Owner (ISO)

The ISO:

- Reviews and updates information system access authorizations for transferred individuals for information systems they own or control.
- Manages opening new accounts and closing old accounts for information systems they own or control.
- Manages changing system authorizations for their information systems.

2.4.3. Center Chief of Security

The Chief of Security or Their Designee:

- Ensures that personnel are properly debriefed, prior to transfer, as appropriate.

2.5. Access Agreements (PS-6)

2.5.1. Information System Owner (ISO)

The ISO:

- Ensures signed access agreements are established, updated, and reviewed in a manner consistent with organizationally defined values.

2.6. External Personnel Security (PS-7)

2.6.1. Center Chief Information Security Officer (Center CISO)

The Center CISO:

- Provides oversight of the logical security implementation of third-party contracts including external/contractor systems at their Center.

2.6.2. Information System Security Officer (ISSO)

The ISSO:

- Provides oversight of the IT security implementation of third-party contracts including external/contractor systems at their organization.

2.6.3. Information System Owner (ISO)

The ISO: * Ensures that contract language specifies that third-party personnel will meet NASA personnel security requirements, including the provision of NASA FAR supplement 1852.204-76, and NPR 1600.1A. ** NASA FAR supplement 1852-204-76 is included in all contracts related to their specific information systems and services.

2.7. Personnel Sanctions (PS-8)

2.7.1. Center Chief Information Security Officer (Center CISO)

The Center CISO or designee:

- Reports cybersecurity security violations at their Center to the appropriate organizations and officials that may need to take security corrective actions.
 - If appropriate for disciplinary or adverse actions, recommendations and actions should be provided in accordance with the NASA Human Capital policies and requirements.
 - If potential for criminal action, information to the Office of the Inspector General (OIG) for investigative and follow-up actions should be provided in accordance with the OIG policies, requirements and procedures.

2.7.2. Enterprise Services and Integration Division

The Enterprise Services and Integration Division:

- Ensures that subscriber agreements signed by an individual to obtain a NASA Public Key Infrastructure (PKI) certificate include the personnel sanctions that may apply for violation of that agreement.
- Ensures formal sanctions are imposed for personnel failing to comply with these information security policies and procedures.
- Reports information security violations by NASA Government or contractor employees to appropriate organizations and officials, and if appropriate to the NASA Security Operations Center (SOC) as a security incident.

APPENDIX A: ACRONYMS

CIO	Chief Information Officer
CISO	[Center] Chief Information Security Officer
CSPD	Cybersecurity and Privacy Division
FAR	Federal Acquisition Regulation
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
HBK	Handbook

HR	Human Resources
IdMAX	Identity Management and Account Exchange
ISO	Information System Owner
ISSO	Information System Security Officer
IT	Information Technology
ITS	Information Technology Security
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
OIG	Office of the Inspector General
PKI	Public Key Infrastructure
SOC	Security Operations Center
SSR	System Security Responsibilities
SP	Special Publication