



IT Security Handbook

Planning -

ITS Handbook (ITS-HBK-2810.03-01)
Planning

Distribution:

NODIS

Approved

Valarie Burks

Valarie Burks
Deputy Chief Information Officer for
Information Technology Security

May 6, 2011

Date

Change History

Version	Date	Change Description
1.0	5/2/11	Initial Document

Table of Contents

Change History	2 -
1 Introduction and Background	4
2 System Security Plan (PL-2).....	4
3 Rules of Behavior (PL-4).....	5
4 Privacy Impact Assessment (PL-5)	5
5 Security-Related Activity Planning (PL-6).....	6
6 Organizationally Defined Values	7

1 Introduction and Background

- 1.1 - 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 (*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, Recommended Security Controls for Federal Information Systems and Organizations*), in a manner consistent with the Risk Management Framework (*NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*).
- 1.2 - 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.
- 1.3 - *NASA Policy Directive (NPD) 2810.1, NASA Information Security Policy, NASA Procedural Requirements (NPR) 2810.1, Security of Information Technology*, and the collection of 2810 Information Technology Handbooks (ITS-HBK) satisfy the policy and procedure controls of *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*.
- 1.4 - *NPR 2810.1, Security of Information Technology*, designates this handbook as a guide of NASA's Planning (PL) information security controls.
- 1.5 - The terms "shall" and "may" within this handbook are used as defined in *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*.
- 1.6 - 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.
- 1.7 - **Applicable Documents**
- *NPD 2810.1, NASA Information Security Policy*
 - *NPR 1382.1, NASA Privacy Procedural Requirements*
 - *NPR 2810.1, Security of Information Technology*
 - *ITS-HBK-0001, Format and Procedures for IT Security Policies and Handbooks*
 - *ITS-HBK-2810.03-02, Planning: Information System Security Plan Template, Requirements, Guidance and Examples*
 - *ITS-HBK-2810-02.07, Security Assessment and Authorization: Information System Security Plan Numbering Schema*
 - *Federal Information Processing Standards (FIPS) 199, Standards for Security Categorization for Federal Information and Information Systems*
 - *FIPS 199, Standards for Security Categorization for Federal Information and Information Systems*
 - *FIPS 200, Minimum Security Requirements for Federal Information and Information Systems*
 - *NIST SP 800-30, Risk Management Guide for Information Technology Systems*
 - *NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*
 - *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*

2 System Security Plan (PL-2)

2.1 - Roles and Responsibilities

2.1.1 - *The Information System Owner (ISO) shall:*

- 2.1.1.1 - Ensure every information system is documented by a System Security Plan (SSP) in the NASA Assessment and Authorization Repository (NSAAR).

- 2.1.1.2 Ensure all SSPs shall have a unique identifier using the NASA standard numbering scheme defined in the *ITS-HBK-2810-02.07, Security Assessment and Authorization: Information System Security Plan Numbering Schema*.
- 2.1.1.3 Ensure all SSPs are reviewed and updated in a manner consistent with organizationally defined values.
 - 2.1.1.3.1 Changes that invalidate already documented controls, control implementations, or risk levels warrant updates to an information system's SSP.
- 2.1.1.4 Ensure all SSPs:
 - 2.1.1.4.1 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;
 - 2.1.1.4.2 Explicitly define the authorization boundary for the system;
 - 2.1.1.4.3 Include a description of the operational environment of the information system in terms of related missions, and business processes;
 - 2.1.1.4.4 Include the security categorization of the information system including supporting rationale;
 - 2.1.1.4.5 Provide an overview of the security requirements for the system; and
 - 2.1.1.4.6 Describe the security controls in place or planned for meeting security requirements, including rational for any tailoring or supplementation of controls.

3 Rules of Behavior (PL-4)

3.1 Roles and Responsibilities

3.1.1 *The ISO shall:*

- 3.1.1.1 Ensure 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)).
- 3.1.1.2 Ensure user accounts are disabled if annual information security training is not completed.
- 3.1.1.3 Establish and implement rules of behavior specific to their system as part of the account management process.

3.1.2 *The Information Technology Security Awareness and Training Center (ITSATC) Project Manager (PM) shall:*

- 3.1.2.1 Ensure that annual information security awareness and training course requires that users acknowledge that they have read, understand, and agree to abide by the rules of behavior prior to authorizing access to NASA information and information systems.

4 Privacy Impact Assessment (PL-5)

4.1 Roles and Responsibilities

4.1.1 *The ISO shall:*

- 4.1.1.1 Ensure an Initial Privacy Threshold Analysis (IPTA) is conducted for all information systems.
 - 4.1.1.1.1 Ensure an IPTA has the concurrence of the Center Privacy Manager and is documented in the SSP.
- 4.1.1.2 Conduct a Privacy Impact Assessment (PIA) in accordance with *NPR 1382.1, NASA Privacy Procedural Requirements*, if the IPTA determination is that a PIA is required.
- 4.1.1.3 Ensure a PIA:
 - 4.1.1.3.1 Has the concurrence of the Center Privacy Manager;
 - 4.1.1.3.2 Has the approval of the Privacy Program Manager and Senior Agency Official for Privacy (SAOP); and
 - 4.1.1.3.3 Is documented in the SSP.

4.1.2 *The NASA SAOP shall:*

- 4.1.2.1 Make approved PIA publicly available through the NASA privacy website.
 - 4.1.2.1.1 The NASA SAOP may determine not to make the full PIA available if sensitive information would be improperly disclosed; in those instances, a summary of such information should be posted.

4.1.3 *The Center Privacy Manager shall:*

- 4.1.3.1 Submit fully completed and signed PIA to the NASA Privacy Program Manager and SAOP for approval.

5 Security-Related Activity Planning (PL-6)

5.1 - NIST guidance is the authoritative source for selection and implementation of this control based on the security categorization and risk environment of the information and/or information system.

6 Organizationally Defined Values

The following table provides the values defined in *NIST SP 800-53* as being at the discretion of the implementing organization. The Section, and Parameter columns are intended to help navigate various *NIST SP 800-53* security controls for easier application of the organizationally defined values; these columns are defined as follows:

- Section: Values in this column indicate whether an organizationally defined value is in the main body of the control (Main), or part of one of the control’s enhancements (E1, E2, etc).
- Parameter: Sometimes, a specific Section may have multiple organizationally defined values. In those instances, the bracketed number Parameters indicate which organizationally defined value (numbered sequentially) is being referenced. In the case of nested organizationally defined values, a series of bracketed numbers is used.

800 53 Reference							FIPS 199 Categorization		
Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
PL	01	Security Planning Policy and Procedures	Main	[1]	Frequency	Policy and procedure review.	1/Year	1/Year	1/Year
PL	02	System Security Plan	Main	[1]	Frequency	System Security Plan review.	1/Year; As governed by Change Management controls	1/Year; As governed by Change Management controls	1/Year; As governed by Change Management controls
PL	02	System Security Plan	E 1	[1]	Frequency	Review of the security CONOPS			