

[| NODIS Library](#) | [Legal Policies\(2000s\)](#) | [Search](#) |

NASA Procedural Requirements

COMPLIANCE IS MANDATORY**NPR 2810.1A**
Effective Date: May 16, 2006
Expiration Date: November
16, 2016[Printable Format \(PDF\)](#)

Request Notification of Change (NASA Only)

Subject: Security of Information Technology (Revalidated with Change 1, dated May 19, 2011)**Responsible Office: Office of the Chief Information Officer**[| TOC](#) | [ChangeHistory](#) | [Preface](#) | [Chapter1](#) | [Chapter2](#) | [Chapter3](#) | [Chapter4](#) | [AppendixA](#) | [AppendixB](#) | [AppendixC](#) | [AppendixD](#) | [AppendixE](#) | [ALL](#) |

Chapter 4 - Technical Controls

4.1 Access Control (AC)

4.1.1 The Access Control security control family relates to the ability of NASA to permit or deny access to computer systems, system locations and system information based on a user's assigned duties. The control family encompasses the management of unique account identifiers (IDs), passwords, physical access, badges and tokens, and user permissions to ensure the proper level of system access.

4.1.2 NASA follows the requirements of HSPD-12, Policies for a Common Identification Standard of Federal Employees and Contractors.

4.1.3 NASA utilizes the guidelines of NIST SP 800-46, Guide to Enterprise Telework and Remote Access Security; NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.

4.1.4 Access Controls procedures shall be governed by NPR 2841.1, Identity, Credential, and Access Management Services; ITS-HBK-2810.15, Access Control; and ITS-HBK-2841-001, Identity, Credential, and Access Management (ICAM) Services Handbook.

4.1.5 Access Control Policy

4.1.5.1 The SAISO shall:

a. Ensure dissemination of the NASA appropriate use policy statement, based on NPD 2540.1, Personal Use of Government Office Equipment Including Information Technology, and the NASA warning banner.

b. Ensure that the NASA warning disclaimer requirements for internal systems are met through the display of the appropriate use and warning banner statements as follows:

1. All computers and applications that are owned by or operated on behalf of NASA and require user authentication for access must display and require acknowledgement of the following NASA warning banner prior to logging on to a NASA system:

This US Government computer is for authorized users only. By accessing this system you are consenting to complete monitoring with no expectation of privacy. Unauthorized access or use may subject you to disciplinary action and criminal prosecution.

2. The following disclaimer is a policy statement which requires concurrence from all users of NASA information systems:

Unauthorized use of the computer accounts and computer resources to which I am granted access is a violation of Federal law; constitutes theft; and is punishable by law. I understand that I am the only individual to access these accounts and will not knowingly permit access by others without written approval. I understand that my misuse of

assigned accounts and my accessing others' accounts without authorization is not allowed. I understand that this/these system(s) and resources are subject to monitoring and recording and I will have no expectation of privacy in my use of and content on these systems and the computer equipment. I further understand that failure to abide by these provisions may constitute grounds for termination of access privileges, administrative action, and/or civil or criminal prosecution.

4.1.5.2 The ISO shall:

- a. Ensure account management capabilities (e.g., account creation, privilege configuration, maintenance, and deletion) are in place for their information systems.
- b. Ensure that accounts for their information systems are administered in a way which provides separation of duties, avoids potential conflicts of interest, and grants NASA users the least privilege necessary to execute their respective duties.
- c. Manage, in collaboration with the IO, access to the information system, and with which privileges users will be authorized.
- d. Ensure the appropriate use and warning banner is displayed by their information system.
- e. Establish documented rules for appropriate use and protection of information (e.g., rules of behavior).

4.1.5.3 The IO shall collaborate with the ISO to manage access to the information system, and with which privileges users will be empowered.

4.1.5.4 The NASA User shall comply with all appropriate use policies.

4.2 Audit and Accountability (AU)

4.2.1 The Audit and Accountability control family relates to the documentation and management of events that occur on or to information system components. Generally, the controls help to answer the questions of "who," "what," "where," "when," and sometimes "how" revolving around various types of information system activities and events (i.e., who logged into a given machine, when, and from where, etc.?). Such audit trails are used for individual accountability, intrusion detection, and problem identification.

4.2.2 Such details are stored in logs which are used to produce useful, actionable information by applying data analysis techniques to detect anomalous trends and patterns that may be cause for concern. The logs can be used both retroactively to determine the causes of an adverse event, and proactively to detect and take action to avoid an imminent adverse event.

4.2.3 Audit and Accountability procedures shall be governed by NPR 1441.1, NASA Records and Retention Schedule; and ITS-HBK-2810.16, Audit and Accountability.

4.2.4 Audit and Accountability Policy

4.2.4.1 The NASA CIO shall ensure the development and maintenance of a capability for the aggregation of NASA-wide information system logs.

4.2.4.2 The SAISO shall:

- a. Ensure that NASA maintains Agency information system record retention policies for logs, and minimum auditable events.
- b. Ensure the development and maintenance of log security auditing capabilities for NASA information system logs.

4.2.4.3 The ISO shall:

- a. Ensure and maintain auditing capabilities for their information system components with consideration given to storage capacity.
- b. Determine the appropriate priorities for audit log events, analysis, and responses. The manner of log collection, extent of the audited events, specific data per event, analysis of the event, and retention times of the audit data will be dependent upon risk levels and the technical capabilities of the components.
- c. Ensure audit logs are strongly controlled, and protected from modification and unauthorized disclosure. This protection should exist throughout the life cycle of the log entry, through creation, transmission, aggregation, reduction, analysis, storage, and disposal.

4.3 Identification and Authentication (IA)

4.3.1 The Identification and Authentication control family relates to the activities and provisions which ensure the identity of a given entity requesting access to NASA resources (e.g., a person logging in to a computer, or a laptop

computer connecting to a wireless network). The controls address the creation, management, usage, and protection of identities (e.g., usernames) and authenticators (e.g., passwords, smart cards, and tokens).

4.3.2 NASA follows the requirements of HSPD-12, Policies for a Common Identification Standard of Federal Employees and Contractors; OMB Memorandum 04-04, E-Authentication Guidance for Federal Agencies; OMB Memorandum 05-24, Implementation of Homeland Security Presidential Directive (HSPD) 12—Policy for a Common Identification Standard for Federal Employees and Contractors; FIPS 140, Security Requirements for Cryptographic Modules; and FIPS 201, Personal Identity Verification (PIV) of Federal Employees and Contractors.

4.3.3 NASA utilizes the guidelines of NIST SP 800-63, Electronic Authentication Guideline.

4.3.4 Identification and Authentication procedures shall be governed by NPR 1600.1, NASA Security Program Procedural Requirements; NPR 2841.1, Identity, Credential, and Access Management Services; ITS-HBK-2810.17, Identification and Authentication ; and ITS-HBK-2841-001, Identity, Credential, and Access Management (ICAM) Services Handbook.

4.3.5 Identification and Authentication Policy

4.3.5.1 The NASA CIO shall provide a NASA-wide framework for identity and authentication management.

4.3.5.2 The ISO shall ensure that applications leverage the Agency identification and authentication framework.

4.3.5.3 The NASA User shall protect identification and authentication information from unauthorized disclosure.

4.3.5.4 The Center Chief of Security or the Assistant Administrator of the Office of Protective Services shall ensure the distribution and management of physical authenticators (e.g., smart cards, and tokens).

4.4 System and Communications Protection (SC)

4.4.1 The System and Communication control family relates to the protection of confidentiality, integrity, and availability of NASA information systems and NASA information as it flows between communications networks. The control family ensures the establishment of an effective physical and logical network security perimeter and provides guidance for best protecting information as it moves both within the security perimeter and as it moves to and from other networks outside the security perimeter such as the Internet.

4.4.2 NASA follows the requirements of X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework; and FIPS 140, Security Requirements for Cryptographic Modules.

4.4.3 System and Communication procedures shall be governed by ITS-HBK-2810.18, System and Communication; and ITS-HBK-2841-001, Identity, Credential, and Access Management (ICAM) Services Handbook.

4.4.4 System and Communications Policy

4.4.4.1 The NASA CIO shall:

- a. Ensure that NASA develops, implements, and maintains Agency common system and communications infrastructure.
- b. Ensure the development and maintenance of a NASA-wide cryptographic key management framework.

4.4.4.2 The Center CIO shall:

- a. Ensure the integration of software and hardware necessary to support system and communications requirements at their Center.
- b. Provision Center-level boundary protection activities for systems which share a common infrastructure and/or services.

4.4.4.3 The ISO shall ensure the implementation of shared resource policies, denial of service protections, boundary protection, and transmission integrity and confidentiality.

[| TOC](#) | [| ChangeHistory](#) | [| Preface](#) | [| Chapter1](#) | [| Chapter2](#) | [| Chapter3](#) | [| Chapter4](#) |
[| AppendixA](#) | [| AppendixB](#) | [| AppendixC](#) | [| AppendixD](#) | [| AppendixE](#) | [| ALL](#) |

[| NODIS Library](#) | [| Legal Policies\(2000s\)](#) | [| Search](#) |

DISTRIBUTION:
NODIS

This Document Is Uncontrolled When Printed.
Check the NASA Online Directives Information System (NODIS) Library
to Verify that this is the correct version before use: <http://nodis3.gsfc.nasa.gov>
