

| [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 3 - Operational Controls

3.1 Awareness and Training (AT)

3.1.1 The Security Awareness and Training control family relates to the information security knowledge requirements for all users of Agency information and information systems, and the development and delivery of courses and other training resources to enable and validate satisfaction of those requirements. Satisfaction of training requirements is a precursor to access controls for NASA information system resources.

3.1.2 Security Awareness and Training procedures shall be governed by ITS-HBK-2810.06, Security Awareness and Training.

3.1.3 Security Awareness and Training Policy

3.1.3.1 The NASA CIO shall:

- a. Develop, maintain, and promote NASA-wide information security awareness and training.
- b. Complete any role-based training activities required of their position.

3.1.3.2 The SAISO shall:

- a. Define and make available all Agency security awareness and training requirements. This includes general knowledge requirements that pertain to all NASA users as well as role-based requirements targeted at managers, information security professionals, etc.
- b. Define educational courses and materials that can be used to satisfy Agency security awareness and training requirements.
- c. Oversee the fulfillment of training requirements across the Agency.
- d. Complete any role-based training activities required of their position.

3.1.3.3 The Center CISO shall:

- a. Track and report on the completion of security awareness and training requirements at the Center level.
- b. Complete any role-based training activities required of their position.

3.1.3.4 The OCSO shall:

- a. Track and report on the completion of security awareness and training requirements at the organizational level.
- b. Complete any role-based training activities required of their position.

3.1.3.5 The ISO shall:

- a. Ensure only users who comply with all Agency information security awareness and training requirements are allowed access to the ISO's information system(s).
- b. Ensure all personnel supporting the information system whose roles include significant information security responsibilities comply with the applicable role-based security awareness and training requirements.
- c. Complete any role-based training activities required of their position.

3.1.3.6 The NASA User shall:

- a. Be responsible for maintaining compliance with applicable security and awareness training requirements, in accordance with role-based security awareness and training requirements.
- b. Ensure their training results are recorded in the designated NASA-wide training platform.

3.1.3.7 The Assistant Administrator of the Office of Human Capital Management shall ensure the availability of a NASA-wide platform for training delivery, as well as training results and records management.

3.2 Configuration Management (CM)

3.2.1 The Configuration Management control family relates to the organizational aspects of information system baseline configurations, establishing review and validation, and change control. The control family also manages administrator roles, and the ability of individuals to make changes to the information systems' configuration.

3.2.2 The concept of configuration management is critical to the continuous monitoring processes. Strict methodologies for the regulation of information system baselines and changes to system configurations are necessary for near real-time understanding of a system's risk posture.

3.2.3 Configuration Management procedures shall be governed by NPR 7120.7, NASA Information Technology and Institutional Infrastructure Program and Project Management Requirements; and ITS-HBK-2810.07, Configuration Management .

3.2.4 Configuration Management Policy

3.2.4.1 The SAISO shall:

- a. Ensure that processes for development, approval, distribution, and verification of security configuration baselines, which are common to all information system components within the Agency, exist and are effective.
- b. Ensure that processes are in place to monitor security baseline configuration compliance.
- c. Ensure security baseline configurations conform to applicable federal requirements (e.g., Federal Desktop Core Configuration (FDCC), United States Government Configuration Baseline (USGCB)).

3.2.4.2 The ISO shall:

- a. Maintain an information system inventory.
- b. Ensure all information system components are incorporated into and maintained in the NASA-wide information system inventory.
- c. Create, implement, and maintain configuration change control policies and processes for their system as needed.
- d. Perform an information system risk analysis to support development of Agency security configuration baselines.

3.2.4.3 The ISSO shall perform an information system risk analysis to justify system configurations and support the process of continuous monitoring.

3.3 Contingency Planning (CP)

3.3.1 The Contingency Planning control family relates to the preparation of information security response, recovery, and continuity activities to avoid disruptions to critical business processes. Successful contingency planning increases the likelihood that essential information and information systems will be available and assists an organization with maintaining continuity of operations in emergency situations. Effective contingency planning, training, testing, and execution are essential to mitigating the impacts resulting from system and service disruptions.

3.3.2 NASA follows the requirements of HSPD-20, National Continuity Policy .

3.3.3 NASA utilizes the guidelines of NIST SP 800-34, Contingency Planning Guide for Information Technology Systems.

3.3.4 Contingency Planning procedures shall be governed by NPR 1040.1, NASA Continuity of Operations Planning

(COOP) Procedures and Guidelines ; and ITS-HBK-2810.08, Contingency Planning.

3.3.5 Contingency Planning Policy

3.3.5.1 The Center CIO shall coordinate Center-wide contingency planning efforts which provide for notification, activation, response, recovery, and reconstitution of a Center's information systems as a result of damage or disruption caused by a man-made or natural disaster.

3.3.5.2 The SAISO shall:

- a. Develop and maintain Agency-level information system contingency planning policies, procedures, and guidance for NASA.
- b. Ensure that NASA has appropriate and tested information security contingency plans in place to continue fulfilling the business functions of NASA in support of the Agency's mission essential functions.
- c. Ensure that Center CISOs are coordinating a Center-based information system contingency program.
- d. Establish recovery metrics and objectives for information systems.
- e. Ensure fulfillment of OMB and FISMA contingency plan testing requirements.

3.3.5.3 The Center CISO shall:

- a. Ensure implementation of those information system contingency planning policies and procedures which provide for notification, activation, response, recovery, and reconstitution.
- b. Oversee and arbitrate conflict resolution for all Center-wide information system contingency plans .
- c. Ensure and support information system contingency plan tests, training, and exercises.

3.3.5.4 The ISO shall:

- a. Be responsible for developing, testing, implementing, and maintaining information system contingency plans.
- b. Ensure that assessment, recovery, and restoration procedures are formally documented.
- c. Be responsible for ensuring that the contingency plan documentation is maintained in a ready state and accurately reflects system requirements, procedures, organizational structure, and policies.
- d. Ensure that recovery and restoration procedures outlined in information system contingency plans satisfy a risk-based analysis of the business needs and objectives of the information system and Agency at large.
- e. Ensure that information system contingency plan documentation is at a level appropriate to permit a coordinated response at the Center and/or the Agency level as applicable.
- f. Be responsible for ensuring that contingency plans are tested, evaluated, and documented appropriately for accuracy, completeness, and effectiveness via a periodic test, training, and exercise program.

3.4 Incident Response and Management (IR)

3.4.1 The Incident Response and Management control family relates to dealing with the potential for and actual damage and disruption to information systems. An "incident" is any adverse event or situation associated with a system that poses a threat to the system's integrity, availability, or confidentiality. An incident may result in or stem from any one of the following: a failure of security controls; an attempted or actual compromise of information; and/or waste, fraud, abuse, loss, or damage of government property or information.

3.4.2 Preventative activities based on the results of risk assessments can lower the number of incidents; however, they will not prevent all incidents. Therefore, an incident response and management capability is necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. The NASA Security Operations Center (SOC) provides centralized Agency coordination for information security incident management, response preparation, identification, analysis, communication, containment, eradication, recovery, and follow-up activities.

3.4.3 NASA utilizes the guidelines of NIST SP 800-61, Computer Security Incident Handling Guide; and NIST SP 800-83, Guide to Malware Incident Prevention and Handling.

3.4.4 Incident Response and Management procedures shall be governed by ITS-HBK-2810.09, Incident Response and Management.

3.4.5 Incident Response and Management Policy

3.4.5.1 The NASA CIO shall allocate resources for a NASA-wide SOC.

3.4.5.2 The Center CIO shall:

- a. Establish an incident response team for their Center.
- b. Ensure capability to support information security investigations.

3.4.5.3 The SAISO shall:

- a. Develop and maintain a NASA-wide process for detecting, reporting, and responding to information security incidents.
- b. Ensure support of investigations into information security incidents conducted by OIG, and the Office of Protective Services (OPS) related to criminal activity, counterintelligence, or counterterrorism.
- c. Ensure support of investigations into information security incidents initiated by the Office of the General Counsel, the office of Human Capital Management, a Center's Office of Human Resources, and a Center's Office of the Chief Counsel.
- d. Refer any suspected criminal, counterintelligence, or counterterrorism activity to the OIG and OPS, respectively, as appropriate.
- e. Implement and manage a NASA-wide SOC.
- f. Oversee all activities related to incident response and management.
- g. Ensure that incidents are appropriately reported to external agencies as directed by applicable laws and regulations.

3.4.5.4 The Center CISO shall:

- a. Provide oversight of the incident response and management policies, procedures, investigations, and reporting for all information systems at their Center.
- b. Provide oversight of the incident response tests, training, and exercises for their Center information systems.
- c. Ensure coordination between the incident response team and the Center privacy managers regarding breach response, and handling of incidents related to sensitive information.

3.4.5.5 The ISO shall:

- a. Designate individuals responsible for incident response reporting and management of their information system.
- b. Ensure that handling of incident information is in accordance with all data sensitivity requirements.
- c. Support information security investigations as appropriate.

3.4.5.6 The ISSO shall ensure effective and timely reporting of all suspected or confirmed security incidents.

3.4.5.7 The NASA User shall report immediately all suspected, or actual, information security incidents to the SOC as outlined in the incident response and management handbook(s).

3.5 Maintenance (MA)

3.5.1 The Maintenance control family relates to the continuous upkeep of information and information systems. In general, maintenance controls are very system specific, and are typically performed based upon vendor recommendations. Many variable factors are considered when making the appropriate maintenance decisions for a system. The business impact, cost, and likelihood of equipment failure, the cost of the maintenance agreement, and the availability of spare equipment can all influence the application of specific Maintenance controls.

3.5.2 NASA recognizes that decisions regarding system specific maintenance requirements are best managed at the information system level, where the specific risks are well understood. However, all Maintenance controls at the information system level must be based on a thorough risk analysis, and accepted risks must be well documented.

3.5.3 Maintenance procedures shall be governed by ITS-HBK-2810.10, Maintenance.

3.5.4 Maintenance Policy

3.5.4.1 The ISO shall:

- a. Develop, maintain, and execute a risk-based maintenance policy and procedures.
- b. Adhere to change control and configuration management processes throughout the life cycle of their information systems.
- c. Maintain oversight of those authorized to perform maintenance on the components of their information system.

3.6 Media Protection (MP)

3.6.1 The Media Protection control family relates to the secure use of information storage media. Storage media can take one of two forms - digital or non-digital. Non-digital media typically consists of paper, film, microfilm, microfiche, etc. Digital media is comprised of mobile computing devices, laptops, personal digital assistants (PDA), "smart phones," and removable storage devices such as USB drives, flash drives, writeable compact discs (CD), and digital video discs (DVD), memory cards, external hard drives, storage cards, diskettes, magnetic tapes, external/removable hard drives, or any electronic device that can be used to copy, save, store and/or move data from one system to another.

3.6.2 The objective of the control family is to prevent or mitigate data loss and/or unauthorized access to NASA information and information systems, due to a failure to secure media, or a failure to sanitize media prior to reuse or disposal.

3.6.3 NASA follows the requirements of FIPS 140, Security Requirements for Cryptographic Modules.

3.6.4 NASA utilizes the guidelines of NIST SP 800-88, Guidelines for Media Sanitization; and NIST SP 800-97, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i.

3.6.5 Media Protection procedures shall be governed by ITS-HBK-2810.11, Media Protection.

a. Special considerations for the use of mobile devices during domestic and international travel are discussed and governed by NPD 2540.1, Personal Use of Government Office Equipment Including Information Technology.

3.6.6 Media Protection Policy

3.6.6.1 The Center CISO shall:

a. Ensure, in coordination with the Center Security Office, that sufficient equipment or services are available to facilitate media sanitization.

b. Ensure that portable and removable digital media devices are guarded using encryption solutions which are compliant with federal encryption algorithm standards and NIST guidance, and are in accordance with NASA requirements regarding the protection of sensitive information.

3.6.6.2 The OCSO shall be responsible for the protection and sanitization of media for their organization. This includes the protection of data at rest.

3.6.6.3 The ISO shall be responsible for the protection and sanitization of media for their information system. This includes the protection of data at rest.

3.6.6.4 The NASA User shall mitigate the risks of data loss by securing and protecting media under their control, and the information contained on/within those devices, through the use of encryption, access restriction, and/or sanitization.

3.6.6.5 The Center Chief of Security or the Assistant Administrator of the Office of Protective Services shall ensure the implementation of media protection security controls.

3.7 Physical and Environmental Protection (PE)

3.7.1 The Physical and Environmental Protection control family relates to the activities and requirements surrounding the development, implementation, and maintenance of physical access authorizations and controls (e.g., key and security badge distribution, visitor management, and related record keeping), and the protection, proofing, and regulation of facilities. NASA protects its facilities and the essential utilities and infrastructure which support those facilities (e.g., door locks, backup power and lighting, emergency plumbing shutoff switches, and fire suppression systems), and also provides appropriate environmental controls for those facilities (e.g., temperature regulation, humidity monitoring). Members of the NASA community are responsible for being aware of, and diligently exercising all facility safety and security procedures.

3.7.2 Physical and Environmental Protection procedures shall be governed by NPR 1600.1, NASA Security Program Procedural Requirements ; NPR 1620.2, Physical Security Vulnerability Risk Assessments ; NPR 1620.3, Physical Security Requirements for NASA Facilities and Property ; NPR 8820, Facility Project Requirements ; NPR 8831.2, Facilities Maintenance and Operations Management ; and ITS-HBK-2810.12, Physical and Environmental Protection.

3.7.3 Physical and Environmental Policy

3.7.3.1 The Center CIO shall work with the Center Chief of Security, and/or the Center Facilities organization to ensure physical and environmental controls are met for the information systems at their Centers.

3.7.3.2 The ISO shall:

- a. Approve personnel need to access secured/restricted physical information system facilities and locations.
- b. Establish and maintain a list of all personnel authorized to access secured/restricted physical information system facilities and locations.
- c. Validate physical and environmental security controls and monitoring capabilities.

3.7.3.3 The Center Chief of Security under the policy guidance of Assistant Administrator of the Office of Protective Services shall:

- a. Ensure the implementation of physical and environmental security controls.
- b. Ensure the capability to monitor physical and environmental security controls.

3.8 Personnel Security (PS)

3.8.1 The Personnel Security control family relates to the 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 applies to both direct employees of the Agency as well as contracted personnel, and service bureaus.

3.8.2 Personnel Security procedures shall be governed by NPD 1600.2, NASA Security Policy; NPD 1600.3, Policy on Prevention of and Response to Workplace Violence ; NPR 2841.1, Identity, Credential, and Access Management Services ; and ITS-HBK-2810.13, Personnel Security.

3.8.3 Personnel Security Policy

3.8.3.1 The SAISO shall ensure that all offices are aware of requirements and expectations related to personnel security.

3.8.3.2 The Center CISO shall confirm that all personnel adhere to the limits of their delegated authority, and act accordingly to address deviations.

3.8.3.3 The ISO shall:

- a. Ensure that all personnel are screened prior to the provision of access to information and information systems.
- b. Ensure that access to secured resources are managed or terminated following the transfer or termination of personnel.

3.8.3.4 The Center Chief of Security under the policy guidance of the Assistant Administrator of Office of Protective Services shall ensure the implementation of personnel security controls.

3.9 System and Information Integrity (SI)

3.9.1 The System and Information Integrity control family relates to the prevention and detection of improper modification or destruction of information or an information system. The control family also includes ensuring the non-repudiation and authenticity of information, as well as flaw remediation (e.g., patching vulnerable software), malicious code prevention (e.g., anti-virus software), and monitoring of attempts to subvert integrity (e.g., an intrusion detection system).

3.9.2 System and Information Integrity procedures shall be governed by ITS-HBK-2810.14, System and Information Integrity.

3.9.3 System and Information Integrity Policy

3.9.3.1 The SAISO shall:

- a. Establish resources for the management of vulnerability, flaw remediation, and information system monitoring.
- b. Ensure the proper handling of vulnerability/patch advisories, including the aggregation of such information from sources both internal and external to the Agency and the Federal government, as well as the wide distribution of such information.
- c. Ensure that the appropriate resources exist to comply with NASA requirements regarding System and Information Integrity including capabilities to detect and prevent the compromise of integrity by known threats (e.g., anti-virus software, block lists) and suspected threats (e.g., automated spam classification and filtering).

3.9.3.2 The Center CISO shall facilitate the implementation of NASA flaw remediation policies and procedures at their Center.

3.9.3.3 The ISO shall:

- a. Ensure that all information system components are identified and documented.
- b. Ensure the completion of flaw remediation activities, and document and communicate residual risks as necessary.
- c. Ensure the implementation of malicious code protections on their information systems.
- d. Ensure that information system security functions are tested in accordance with requirements, and that the frequency and processes related to the tests are formally documented.

| [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>
