



IT Security Handbook

Incident Response and Management

ITS-HBK-2810.09-01
Effective Date: 20110506
Expiration Date: 20130506
Responsible Office: OCIO/ Deputy CIO for Information Technology Security

ITS Handbook (ITS-HBK-2810.09-01)
Incident Response and Management

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 Draft

Table of Contents

Change History	3 -
1 Introduction and Background	5 -
2 Incident Response Training (IR-2)	5 -
3 Incident Response Testing and Exercises (IR-3)	6 -
4 Incident Handling (IR-4)	6 -
5 Incident Monitoring (IR-5)	7 -
6 Incident Reporting (IR-6).....	7 -
7 Incident Response Assistance (IR-7)	8 -
8 Incident Response Plan (IR-8)	8 -
9 Organizationally Defined Values.....	9 -

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 Incident Management (IR) 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 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.
- 1.7 - Preventative activities based on the results of risk assessments can lower the number of incidents, however they may not prevent all incidents. Therefore, an incident management capability is necessary for rapidly handling incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring computing services. The Security Operations Center (SOC) provides centralized Agency oversight for information security incident management, response preparation, identification, analysis, and communication.
- 1.8 - **Applicable Documents**
- *NPD 2810.1, NASA Information Security Policy*
 - *NPR 2810.1, Security of Information Technology*
 - *ITS-HBK-0001, Format and Procedures for an IT Security Handbook*
 - *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 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems*
 - *NIST SP 800-53, Recommended Security Controls for Federal Information Systems and Organizations*
 - *NIST SP 800-61, Computer Security Incident Handling Guide*
 - *NIST SP 800-83, Guide to Malware Incident Prevention and Handling*

2 Incident Response Training (IR-2)

- 2.1 - **Roles and Responsibilities**
- 2.1.1 *The Senior Agency Information Security Officer (SAISO) shall:*

2.1.1.1 Ensure funding and support of incident response training activities in a manner consistent with organizationally defined values.

2.1.2 *The Security Operations Center (SOC) shall:*

2.1.2.1 Establish procedures for supporting general NASA incident response training in a manner consistent with organizationally defined values.

2.1.2.2 Ensure that all incident responders are trained on their incident response roles and responsibilities.

2.1.2.3 Assist the Information Technology Security Awareness and Training Center (ITSATC) with the development of incident response training.

2.1.2.3.1 Refresher training shall be conducted in a manner consistent with organizationally defined values.

2.1.2.3.2 Training should include simulated events to facilitate effective response in a crisis situation.

2.1.2.4 Ensure that lessons learned from on-going incident handling activities are incorporated into incident response training.

3 Incident Response Testing and Exercises (IR-3)

3.1 Roles and Responsibilities

3.1.1 *The SAISO shall:*

3.1.1.1 Review and approve incident response testing and exercise activities.

3.1.2 *The SOC shall:*

3.1.2.1 Establish procedures for supporting incident response testing and exercises.

3.1.2.1.1 Incident response tests and exercises shall be conducted in a manner consistent with organizationally defined values.

3.1.2.1.2 Incident response tests and exercises should include scenarios validating the procedures established in accordance with SOC incident response training procedures.

3.1.2.2 Ensure that lessons learned from on-going incident handling activities are incorporated into incident response testing/exercises.

4 Incident Handling (IR-4)

4.1 Roles and Responsibilities

4.1.1 *The Center Chief Information Security Officer (CISO) shall:*

4.1.1.1 Provide oversight for the incident response policies, procedures, investigations, and reporting of Center incidents.

4.1.1.2 Establish an interview process for Incident Responders to follow to determine what information systems and related components have been potentially affected by a suspected incident.

4.1.2 *The Organization Computer Security Official (OCSO) shall:*

4.1.2.1 Provide oversight for the incident response policies, procedures, investigations, and reporting of organizational incidents.

4.1.3 *The ISO shall:*

4.1.3.1 Ensure incident handling activities are coordinated with, and included in, contingency planning activities.

4.1.4 *The SOC shall:*

4.1.4.1 Maintain an Agency Incident Management System (IMS).

4.1.4.2 Ensure that handling procedures and capabilities are implemented for analysis, and reporting of information system incidents.

4.1.4.3 Ensure that lessons learned from on-going incident handling activities are incorporated into incident response procedures.

- 4.1.5 *The Incident Responder shall:* -
 - 4.1.5.1 - Notify the SOC of the status of reported incidents. -
 - 4.1.5.2 - Confirm incidents as reported by various sources. -
 - 4.1.5.3 - Complete incident response documentation regarding: -
 - 4.1.5.3.1 The nature of information on affected systems (e.g., ITAR, PII); -
 - 4.1.5.3.2 Estimated costs of response; and -
 - 4.1.5.3.3 Estimated impacts to user (e.g., system downtime, loss of productivity). -
 - 4.1.5.4 - Ensure completion and closure of incidents within a timely manner. -
 - 4.1.5.4.1 Incidents which cannot be closed within 30 days shall be reassigned as “Under Investigation”. -
 - 4.1.5.5 - Ensure delivery of digital media to the SOC for analysis, as necessary. -

5 Incident Monitoring (IR-5)

5.1 Roles and Responsibilities

- 5.1.1 *The SOC shall:* -
 - 5.1.1.1 - Ensure information system security incidents are tracked and documented in the Agency IMS. -
 - 5.1.1.2 - Ensure relevant data from all available information sources (e.g., audit monitoring, network monitoring, application logs) are included in incident documentation through the Agency IMS. -

6 Incident Reporting (IR-6)

6.1 Roles and Responsibilities

- 6.1.1 *The SAISO shall:* -
 - 6.1.1.1 - Ensure that the release of incident information to those outside of Center security personnel, Center Chief of Security (CCS), Office of Protective Services (OPS), the Office of the Inspector General (OIG), US-CERT and other Agency CERTS, is handled only by the NASA Headquarters Public Affairs Office (PAO). -
- 6.1.2 *The ISO shall:* -
 - 6.1.2.1 - Report actual or suspected information security incidents regarding information systems under their purview - immediately to the SOC or appropriate organization (e.g., Center-specific IT Security office, incident response team, or help desk). -
 - 6.1.2.2 - Report actual or suspected misuse of IT resources to the SOC, Center CISO or other appropriate organizations (e.g., Center-specific IT security office, incident response team, or help desk). -
- 6.1.3 *The NASA User shall:* -
 - 6.1.3.1 - Report actual or suspected information security incidents immediately to the NASA SOC. -
 - 6.1.3.2 - Report actual or suspected misuse of IT resources to the SOC, Center CISO, or other appropriate officials. -
- 6.1.4 *The SOC shall:* -
 - 6.1.4.1 - Ensure reporting capabilities of incident management information. -
 - 6.1.4.2 - Serve as the Agency interface to US-CERT and other Agency CERTS. -
 - 6.1.4.3 - Ensure that incidents are securely reported to the US-CERT and other designated agencies/organizations/authorities in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards and guidance. -
 - 6.1.4.4 - Ensure reporting of incidents of actual or suspected misuse of IT resources to the appropriate NASA authorities. -
 - 6.1.4.5 - Ensure the availability of SOC capabilities in support of incident reporting on a 24x7x365 basis. -

7 Incident Response Assistance (IR-7)

- 7.1 - 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. -

8 Incident Response Plan (IR-8)

8.1 - Roles and Responsibilities

8.1.1 *The SAISO shall:* -

- 8.1.1.1 Serve as the approval authority of the NASA Incident Response Plan. -
- 8.1.1.2 Ensure dissemination of the Incident Response Plan to: -
 - 8.1.1.2.1 - Center CISOs; -
 - 8.1.1.2.2 - Center Information Security Incident Response Managers; -
 - 8.1.1.2.3 - Individuals identified as Incident Responders; and -
 - 8.1.1.2.4 - Managers of activities and facilities that may be impacted by the Incident Response Plan. -

8.1.2 *The Center CISO shall:* -

- 8.1.2.1 Ensure the development of incident response capabilities at their Center. -

8.1.3 *The Agency Incident Response Manager (AIRM) shall:* -

- 8.1.3.1 Ensure the development of an Incident Response Plan that: -
 - 8.1.3.1.1 - Provides a high-level approach for how the incident response capability fits into the overall agency. -
 - 8.1.3.1.2 - Meets the unique requirements of the agency, which relate to mission, size, structure, and functions. -
 - 8.1.3.1.3 - Provides metrics for measuring the incident response capability within the agency. -
 - 8.1.3.1.4 - Defines the resources and management support needed to effectively maintain and mature an incident response - capability. -

9 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.

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
IR	01	Incident Response Policy and Procedures	Main	[1]	Frequency	Policy and procedure review.	1/Year	1/Year	1/Year
IR	02	Incident Response Training	Main	[1]	Frequency	Incident response refresher training.	1/Year	1/Year	1/Year
IR	03	Incident Response Testing and Exercises	Main	[1]	Frequency	Tests/exercises of incident response capabilities.	1/Year	1/Year	1/Year
IR	03	Incident Response Testing and Exercises	Main	[2]	Reference	List of tests/exercises.	SOC-Defined	SOC-Defined	SOC-Defined
IR	04	Incident Handling	E 5	[1]	Reference	List of security violations which trigger automatic disabling of an information system upon detection.			
IR	06	Incident Reporting	Main	[1]	Time Period	Elapse between discovery and reporting of suspected security incidents.	Immediate	Immediate	Immediate

ITS Handbook (ITS-HBK-2810.09-01) -
Incident Response and Management -

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
IR	08	Incident Response Plan	Main	[1]	Reference	List of incident response personnel to whom copies of the incident response plan is distributed.	a. Center CISO (Information Technology Security Manager) b. Center information Security Incident Response Manager. c. Individuals that are indentified in the plan for incident response actions. d. Managers of activities and/or facilities that may be impacted by the plan.	a. Center CISO (Information Technology Security Manager) b. Center information Security Incident Response Manager. c. Individuals that are indentified in the plan for incident response actions. d. Managers of activities and/or facilities that may be impacted by the plan.	a. Center CISO (Information Technology Security Manager) b. Center information Security Incident Response Manager. c. Individuals that are indentified in the plan for incident response actions. d. Managers of activities and/or facilities that may be impacted by the plan.
IR	08	Incident Response Plan	Main	[2]	Frequency	Incident response plan review.	1/Year	1/Year	1/Year

ITS Handbook (ITS-HBK-2810.09-01) -
Incident Response and Management -

Family	#	Name	Section	Parameter	Type	Description	Low	Moderate	High
IR	08	Incident Response Plan	Main	[3]	Reference	Distribution list for changes to incident response plan.	a. Center CISO (Information Technology Security Manager) b. Center information Security Incident Response Manager. c. Individuals that are indentified in the plan for incident response actions. d. Managers of activities and/or facilities that may be impacted by the plan.	a. Center CISO (Information Technology Security Manager) b. Center information Security Incident Response Manager. c. Individuals that are indentified in the plan for incident response actions. d. Managers of activities and/or facilities that may be impacted by the plan.	a. Center CISO (Information Technology Security Manager) b. Center information Security Incident Response Manager. c. Individuals that are indentified in the plan for incident response actions. d. Managers of activities and/or facilities that may be impacted by the plan.