



**NASA TECHNICAL HANDBOOK**

**National Aeronautics and Space Administration**

**ITS-HBK-2810.09-01 v2024-02**

**Published: 2024-02-23**

**Incident Response and Management  
TECHNICAL HANDBOOK**

# TABLE OF CONTENTS

|                                                                     |   |
|---------------------------------------------------------------------|---|
| Document Properties                                                 | 3 |
| Document History Log                                                | 3 |
| Approval                                                            | 3 |
| 1. Introduction                                                     | 4 |
| 1.1. Scope                                                          | 4 |
| 1.2. Point of Contact(s)                                            | 4 |
| 1.3. Applicability                                                  | 4 |
| 1.4. Applicable Documents                                           | 4 |
| 1.4.1. Federal Information Processing Standards (FIPS)              | 5 |
| 1.4.2. National Institute of Standards and Technology (NIST)        | 5 |
| 1.4.3. National Aeronautics and Space Administration (NASA)         | 5 |
| 2. Incident Response Training ( <a href="#">IR-2</a> )              | 5 |
| 2.1. Roles and Responsibilities                                     | 5 |
| 2.1.1. Senior Agency Information Security Officer (SAISO)           | 5 |
| 2.1.2. Security Operations Center (SOC)                             | 5 |
| 3. Incident Response Testing and Exercises ( <a href="#">IR-3</a> ) | 6 |
| 3.1. Roles and Responsibilities                                     | 6 |
| 3.1.1. Senior Agency Information Security Officer (SAISO)           | 6 |
| 4. Incident Handling ( <a href="#">IR-4</a> )                       | 6 |
| 4.1. Roles and Responsibilities                                     | 6 |
| 4.1.1. Center Chief Information Security Officer (CISO)             | 6 |
| 4.1.2. Organization Computer Security Official (OCSO)               | 6 |
| 4.1.3. Information System Owner (ISO)                               | 6 |
| 4.1.4. Security Operations Center (SOC)                             | 6 |
| 4.1.5. Incident Responder                                           | 7 |
| 5. Incident Monitoring ( <a href="#">IR-5</a> )                     | 7 |
| 5.1. Roles and Responsibilities                                     | 7 |
| 5.1.1. Security Operations Center (SOC)                             | 7 |
| 6. Incident Reporting ( <a href="#">IR-6</a> )                      | 7 |
| 6.1. Roles and Responsibilities                                     | 7 |
| 6.1.1. Senior Agency Information Security Officer (SAISO)           | 7 |
| 6.1.2. Information System Owner (ISO)                               | 7 |
| 6.1.3. NASA User                                                    | 8 |
| 6.1.4. Security Operations Center (SOC)                             | 8 |
| 7. Incident Response Assistance ( <a href="#">IR-7</a> )            | 8 |
| 8. Incident Response Plan ( <a href="#">IR-8</a> )                  | 8 |
| 8.1. Roles and Responsibilities                                     | 8 |
| 8.1.1. Senior Agency Information Security Officer (SAISO)           | 8 |
| 8.1.2. Center Chief Information Security Officer (CISO)             | 9 |
| 8.1.3. Agency Incident Response Manager (AIRM)                      | 9 |
| 9. Organization-Defined Values                                      | 9 |
| Appendix A: Acronyms                                                | 9 |

# 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, and the NIRWG handbook is updated. |
| 1.3              | 2014-12-04     | Extended for updates and revisions                                                                 |
| 1.4              | 2018-06-15     | Extended for updates and revisions                                                                 |
| 1.5              | 2019-11-06     | Reformatting and minor updates                                                                     |
| 1.6              | 2021-09-30     | Updated with NIST SP Rev. 5 provisions.                                                            |
| 1.7              | 2023-01-31     | Annual update.                                                                                     |
| v2023-12         | 2023-12-18     | Updated to new format                                                                              |
| v2024-02         | 2024-02-23     | Annual update                                                                                      |

## Approval

# 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 shall follow NIST guidance in the proper security categorization ([FIPS 199, \*Standards for Security Categorization of 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 SP 800-53, \*Security and Privacy Controls for Information Systems and Organizations\*](#)), in a manner consistent with the Risk Management Framework ([NIST SP 800-37, \*Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy\*](#)). 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.

NPD 2810.1, [NASA Information Security Policy](#), 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 [SP 800-53](#). NPR 2810.1, [Security of Information and Information Systems](#), designates this handbook as a guide of NASA's Incident Management (IR) information security controls. The content of this document, in conjunction with NPD/R 2810.1, defines NASA policy and procedures to address [IR-1](#).

## 1.1. Scope

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. 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.

## 1.2. Point of Contact(s)

For any questions or comments regarding the contents of this Handbook, contact:

- [hq-dl-cspd-policy@mail.nasa.gov](mailto:hq-dl-cspd-policy@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 shall be elevated to the NASA CSPD, in coordination with the CISO, and directed to the attention of the point of contact for this Handbook to address and resolve.

## 1.3. 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.

## 1.4. Applicable Documents

### 1.4.1. 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*

### 1.4.2. National Institute of Standards and Technology (NIST)

- NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*
- NIST SP 800-61, *Computer Security Incident Handling Guide*
- NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- NIST SP 800-83, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*

### 1.4.3. National Aeronautics and Space Administration (NASA)

- NPD 2810.1, *NASA Information Security Policy*
- NPR 2810.1, *Security of Information and Information Systems*
- NASA-SPEC-2661.ODVr5, *NASA's Organization-Defined Values for NIST SP 800-53 Revision 5*

## 2. INCIDENT RESPONSE TRAINING (IR-2)

### 2.1. Roles and Responsibilities

#### 2.1.1. Senior Agency Information Security Officer (SAISO)

*The Senior Agency Information Security Officer (SAISO) shall:*

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

#### 2.1.2. Security Operations Center (SOC)

*The Security Operations Center (SOC) shall:*

- Establish procedures for supporting general NASA incident response training in a manner consistent with organizationally defined values.
- Ensure that all incident responders are trained on their incident response roles and responsibilities.
- Assist the Information Technology Security Awareness and Training Center (ITSATC) with the development and update of incident response training.
  - Refresher training shall be conducted in a manner consistent with organizationally defined values.
  - Training should include simulated events to facilitate effective response in a crisis situations.
- 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. Senior Agency Information Security Officer (SAISO)

*The SAISO shall:*

- Establish procedures for supporting incident response testing and exercises.
  - Incident response tests and exercises shall be conducted in a manner consistent with organizationally defined values.
  - Incident response tests and exercises should include scenarios validating the procedures established in accordance with SOC incident response training procedures.
  - 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. Center Chief Information Security Officer (CISO)

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

- Provide oversight for the incident response policies, procedures, investigations, and reporting of Center incidents.
- 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. Organization Computer Security Official (OCSO)

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

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

#### 4.1.3. Information System Owner (ISO)

*The ISO shall:*

- Ensure incident handling activities are coordinated with, and included in, contingency planning activities.
- Ensure the development of a system-specific incident response plan to ensure users contact the SOC to report cybersecurity incidents.

#### 4.1.4. Security Operations Center (SOC)

*The SOC shall:*

- Maintain an Agency Incident Management System (IMS).
- Ensure that handling procedures and capabilities are implemented for analysis and reporting of information system incidents.
- Ensure that lessons learned from on-going incident handling activities are incorporated into incident response procedures.

#### **4.1.5. Incident Responder**

*The Incident Responder shall:*

- Notify the SOC of the status of reported incidents.
- Confirm incidents as reported by various sources.
- Complete incident response documentation regarding:
  - The nature of information on affected systems (e.g., ITAR, PII);
  - Estimated costs of response; and
  - Estimated impacts to users (e.g., system downtime, loss of productivity).
- Ensure completion and closure of incidents within a timely manner.
  - Incidents which cannot be closed within 30 days shall be reassigned as “Under Investigation”.
- 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. Security Operations Center (SOC)**

*The SOC shall:*

- Ensure cybersecurity and privacy incidents are tracked and documented in the Agency IMS.
- 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. Senior Agency Information Security Officer (SAISO)**

*The SAISO shall:*

- 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. Information System Owner (ISO)**

*The ISO shall:*

- Report actual or suspected cybersecurity 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).
- 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. NASA User

*The NASA User shall:*

- Report actual or suspected incidents immediately to the NASA SOC.
- Report actual or suspected misuse of IT resources to the SOC, Center CISO, or other appropriate officials.

### 6.1.4. Security Operations Center (SOC)

*The SOC shall:*

- Ensure reporting capabilities of incident management information.
- Serve as the Agency interface to US-CERT and other Agency CERTS.
- 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.
- Ensure reporting of incidents of actual or suspected misuse of IT resources to the appropriate NASA authorities.
- Ensure the availability of SOC capabilities in support of incident reporting on a 24x7x365 basis.

## 7. INCIDENT RESPONSE ASSISTANCE (IR-7)

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. Senior Agency Information Security Officer (SAISO)

*The SAISO shall:*

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

### 8.1.2. Center Chief Information Security Officer (CISO)

*The Center CISO shall:*

- Ensure the contact information for the SOC is available, with instructions for users to contact the SOC for all cybersecurity-related incidents. Ensure the development of a system-specific incident response plan to ensure users contact the SOC to report cybersecurity incidents.

### 8.1.3. Agency Incident Response Manager (AIRM)

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

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

## 9. ORGANIZATION-DEFINED VALUES

NASA's Organization-Defined Values (ODVs) for security controls defined in [SP 800-53](#) as being at the discretion of the implementing organization are listed in [NASA-SPEC-2661.ODVr5](#), [NASA's Organization-Defined Values for NIST SP 800-53 Revision 5](#).

## APPENDIX A: ACRONYMS

|              |                                                |
|--------------|------------------------------------------------|
| <b>CISO</b>  | Center Chief Information Security Officer      |
| <b>FIPS</b>  | Federal Information Processing Standards       |
| <b>FISMA</b> | Federal Information Security Management Act    |
| <b>HBK</b>   | Handbook                                       |
| <b>IMS</b>   | Incident Management System                     |
| <b>ISO</b>   | Information System Owner                       |
| <b>ISSO</b>  | Information System Security Officer            |
| <b>IT</b>    | Information Technology                         |
| <b>ITAR</b>  | International Traffic in Arms                  |
| <b>NASA</b>  | National Aeronautics and Space Administration  |
| <b>NIST</b>  | National Institute of Standards and Technology |
| <b>NPD</b>   | NASA Policy Directive                          |

|              |                                            |
|--------------|--------------------------------------------|
| <b>NPR</b>   | NASA Procedural Requirement                |
| <b>OCSO</b>  | Organization Computer Security Official    |
| <b>PII</b>   | Personally Identifiable Information        |
| <b>PAO</b>   | Public Affairs Office                      |
| <b>SAISO</b> | Senior Agency Information Security Officer |
| <b>SOC</b>   | Security Operations Center                 |
| <b>SP</b>    | Special Publication                        |