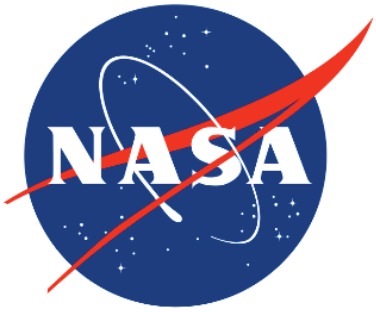


Information Technology Security Handbook

Incident Response and Management: Guidelines for Data Spillage and Sanitization Procedures

November 2023

Version 3.0

OFFICE OF THE CHIEF INFORMATION OFFICER

CYBER SECURITY AND PRIVACY DIVISION

Document Properties

- **Maintained by**: OCIO CSPD Team
- **Filename**: ITS-HBK-2810.09-04A Incident Response and Management: Guidelines for Data Spillage and Sanitization Procedures
- **Supersedes:**
  Version 2.0

Table 1: Revision History

Version	Date	Change Description
1.0	02/27/2014	Initial draft.
2.0	11/6/2019	Reformatting and minor updates.
3.0	11/3/2023	General review and alignment with OCIO transformation process. Clarification between Spillage procedures and Collection of Electronic Data procedures.

Table of Contents

1. Introduction 1
1.1 Purpose 1
1.2 Scope 1
1.3 Point of Contact(s) 1
1.4. Applicability 1
1.5. Applicable Documents 2
2. Roles and Responsibilities 2
3. Data Spillage Process Overview 4
Phase 1 - Notification 5
Phase 2 – Response 6
3.1. The Data Spillage Response Team will address, at a minimum, the 6
following questions: 6
3.2. Selection of the appropriate remediation procedure is dependent on 6
several factors that may include: 6
3.3 Risk Assessment. 7
Phase 3 – Final Adjudication 7
Appendix A: Acronyms 8
Appendix B: Incident Action Examples 10
Incident Action Example 10
Actions 10

This page intentionally left blank.

Distribution:

NODIS

Approved



Associate Chief Information Officer
for Cybersecurity & Privacy

1. Introduction

The National Aeronautics and Space Administration (NASA) adheres to the guidance National Institute of Standards and Technology (NIST) and internal policies to outline the responsibilities of all parties involved in a data spillage response. NASA Policy Directive (NPD) 2810.1 NASA Information Security Policy and NPR 2810.1 Security of Information and Information Systems and Information together with other 2810 family of technology handbooks designate this handbook as a guide of NASA's data spillage. It also augments NIST guidance with NASA-specific requirements, procedures, and recommendations, where applicable.

1.1 Purpose

The purpose of this handbook is to document the responsibilities for anyone in charge of the implementation of this handbook and ensure they have a full and complete understanding of their roles and responsibilities.

1.2 Scope

Data spillage is a security incident where information is placed on systems that are not authorized to process such information. Information spills occur when information that is thought to be a certain classification or impact level is transmitted to a system and subsequently is determined to be of a higher classification or impact level. Corrective actions are based on the nature of the response, classification, and the spilled information, the security capabilities of the system, the specific nature of the contaminated storage media, and the access authorizations of individuals with authorized access to the contaminated system. The Security Operations Center (SOC) in conjunction with other offices provides centralized Agency oversight for information security incident management, response preparation, identification, analysis, and communication.

1.3 Point of Contact(s)

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

OCIO Policy Team

- 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.

1.4. 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 (JPL), 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.

1.5. Applicable Documents

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88, Guidelines for Media Sanitization
- NIST 800-53, Security and Privacy Controls for Information and Information Systems
- Securing Data and Handling Spillage Events: The Information Assurance Mission at NSA, October, 2012
- Frequently Asked Questions on Incidents and Spills, CNSS-079-07
- NASA Procedural Requirement (NPR) 1600.2, NASA Classified National Security Information
- ITS-HBK-2810.09-01, Incident Response and Management
- ITS-HBK-2810.09-02, Incident Response and Management: NASA Information Security Incident Management

2. Roles and Responsibilities

The NASA OCIO shall:

- Collaborate with OPS to develop and test data spillage procedures.
- Ensure that the NASA Security Operations Center (SOC) is prepared to support agency data spillage.
- Provide an official with the appropriate clearance level to support the data spillage team.
- Collaborate on after action reports (AARs).
- Ensure that data spillage procedures are incorporated into the enterprise services contract.
- Ensure that enterprise systems (email, etc.) have the appropriate *NIST SP 800-53* security controls in place to support a data spillage that involves all levels of information classification.
- Provide oversight on all data spillage remediation efforts involving enterprise services contracts.
- Ensure that the enterprise services contract provider properly sanitizes media prior to removal from agency inventory.

The Center CISO shall:

- Collaborate on AARs.

The NASA SOC shall:

- Provide an official and staff with the appropriate clearance level to support the Data Spillage Response Team.
- Ensure that all known or suspected instances of data spillages of classified information are promptly investigated pursuant to their areas of responsibilities.
- Ensure notification of the data spillage to the responsible official within the OCIO and OPS.
- Notify and coordinate response with Center CISO, Cyber Incident Response Team (CIRT), and other stakeholders, as appropriate.
- Track and report the activity as needed for situational awareness.

- Collaborate on AARs.

The CIRT shall:

- Follow the responsibilities outlined in *ITS-HBK-2810.09-02*.
- Ensure appropriate actions are taken to isolate and contain the data spillage, as well as to preclude unauthorized access, while using risk management principles to maintain continuity of operations.
- Oversee the appropriate procedures for sanitizing or remediating the effects of a data spill.
- In coordination with associated Cybersecurity Risk Manager(s) (CSRM) ensure that all follow-up activities are conducted, e.g., work to strengthen security controls, or weaknesses, that allowed the incident to occur with the coordination of OPS.
- Refer information security incidents that are determined to be computer crimes immediately to the Assistant Administrator, Office of Protective Services for disposition and/or report them to the Office of the Inspector General (OIG) for investigation, as appropriate.
- Support the OIG investigation of computer crimes, if requested by the OIG.

Workplace Collaboration Services (WCS) shall:

- Assist the Data Spillage Response Team (provided the WCS representative has the appropriate security clearance level to support) for WCS-managed systems and services.
- Receive and respond to end user device data spillage notifications.

The NASA HQ OPS shall:

- Assemble the investigative team and oversee and monitor the investigation of data spillages of CNSI.
- Ensure that the responsible official and all supporting personnel have the appropriate clearance level to support the data spillage.
- Provide direction for reporting and investigating data spillage of CNSI onto an unclassified information system, or higher-level classified information onto lower-level classified information system or onto a system not accredited to that category of information, to include non-government systems.
- Review findings of initial inquiry and/or investigation of data spillages of CNSI.
- Ensure all incidents related to CNSI are appropriately reported, prioritized, categorized, tracked, assigned, and documented in the Incident Management System (IMS), incorporating impact and damage assessments.
- Determine whether an additional internal investigation is appropriate, depending on the results of the initial inquiry and/or investigation. Consultation should take place with the department/agency that possesses original classification authority for the information.
- Determine whether the incident should be referred to law enforcement for investigation and/or criminal prosecution.
- Notify the Administrator, Deputy Administrator, and the OCIO, as required.
- Request the initiation of comprehensive analyses and damage assessments when such disclosures affect International Traffic in Arms Regulations (ITAR) information, intelligence or counterintelligence activities, capabilities, and techniques.

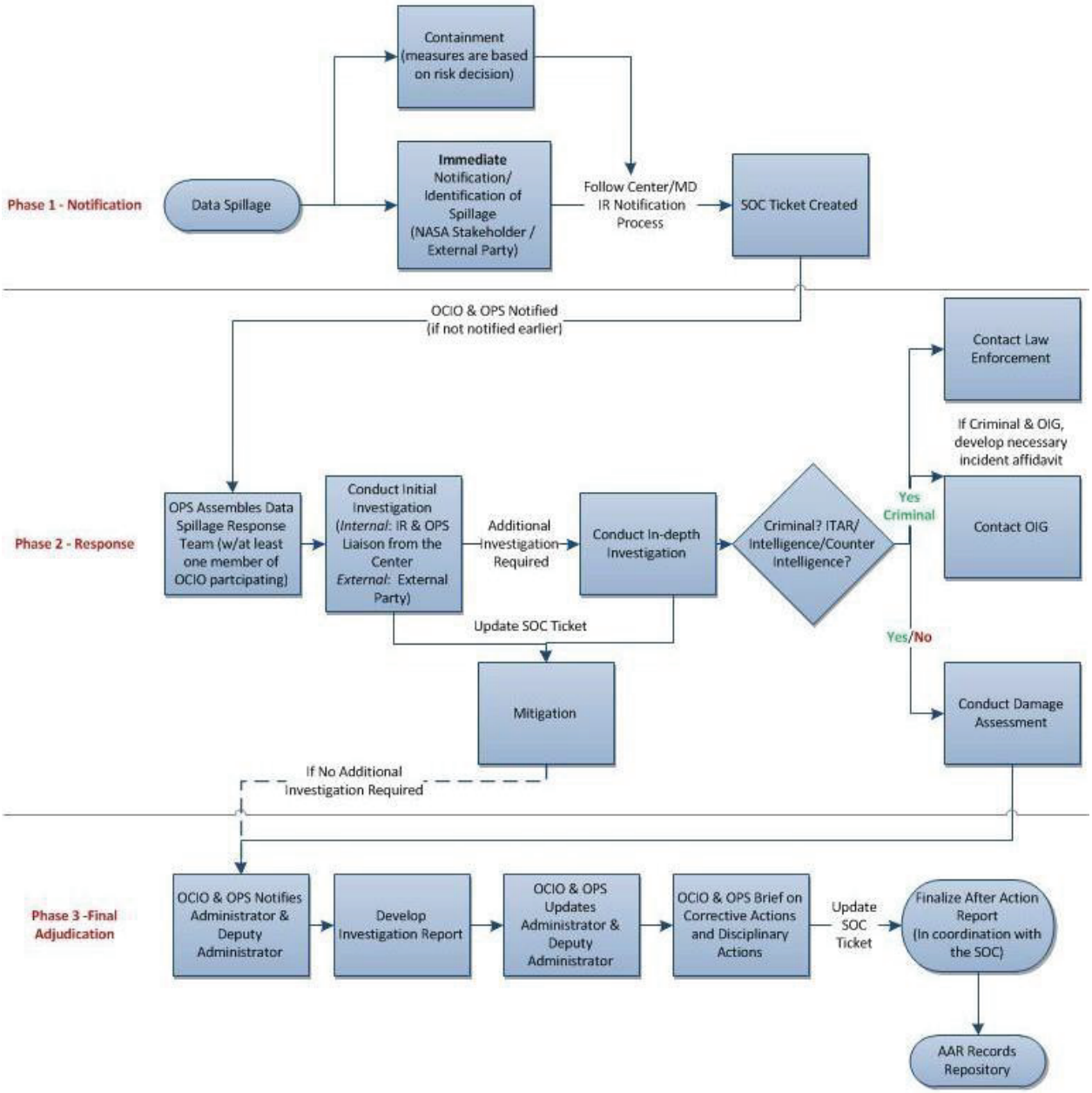
- Provide a final after-action report to the OCIO, SOC, and other parties once all remediation actions are complete.
- Report the investigative results and any corrective and/or disciplinary action taken to the department/agency head, in collaboration with OCIO.
- Provide follow-up security education and awareness to all briefed and uncleared personnel involved.
- Ensure training for the handling of classified information is conducted with the end user.
- Designate, at their discretion, a responsible official for implementing the responsibilities listed above.

The Information Owner/Data Owner shall:

- Have operational authority for specified information.
    - Note: The Information Owner/Data Owner may be an organization or individual(s).

3. Data Spillage Process Overview

The chart on the following page provides a basic overview of the Data Spillage process:



Phase 1 - Notification

Upon determination that a data spillage has occurred, a formal inquiry shall be conducted. As per *ITS-HBK-2810.09-01* Organizationally Defined Values (ODVs), the Data Spillage Response Team shall be notified immediately to investigate the data spillage. Individuals that are dealing with the IR will make a risk-based decision about appropriate containment measures. Based on the kind of spillage, the Data Spillage Response Team shall: act simultaneously between containment and notification, either choosing to contain, and then notify, or immediately notify first and then contain, followed by the next process.

At a minimum, the Data Spillage Response Team shall include the related NASA Stakeholder, the

External Party, the OCIO representative, and OPS. In addition, the team may include the OIG, Center CISO, Information System Security Officer (ISSO), Center Operation Security Manager (OSM), Information Owner, and law enforcement authorities, as appropriate. Finally, the NASA SOC coordinates the response with the Center CISO, IRM, and other stakeholders.

Phase 2 – Response

The OPS coordinates with at least one participating member of OCIO to assemble the Data Spillage Response Team and conducts the initial investigation (internally with IR and OPS Liaison from the Center and externally with external party).

3.1. The Data Spillage Response Team will address, at a minimum, the following questions:

1. When did the data spillage occur?
2. What data was spilled?
3. Who is the data owner?
4. What was the classification/category of the spilled data or information?
5. Was the classified information in question properly classified?
6. What steps were taken to contain the data spillage?
7. What caused the data spillage to occur?
8. Who was responsible for the data spill?
9. What was the flow of information to reach its ultimate destination (e.g., specific mail, file servers, or removable media)?
10. Was the information in question printed?
11. Where is the information now stored (information system(s) and printed material)?
12. What steps were taken to identify the person(s) responsible for the data spillage?
13. What individuals had access to the information and what was their clearance level?
14. In what specific media did the classified information originate?
15. What information system(s) were affected and to what extent?
16. Will further inquiry increase the damage caused in the event of a clean-up?
17. Is the information being handled as evidence?

3.2. Selection of the appropriate remediation procedure is dependent on several factors that may include:

- The difference between the classification and category of the spilled information and the classification and category approved for the system containing the spilled information.
- The requirements of the information owner regarding information sensitivity and risks from inadvertent disclosure.
- Financial considerations, including costs of media replacement and resources required for remediating the spill.
- Operation and mission impacts.

- Pre-existing agreements between the Information Owner's and the spiller's organization(s).
- Assessment of the effectiveness of the sanitization/remediation procedures. Unless otherwise determined by the information owner, in cases where the spillage occurred within agency-controlled space, sanitization is not required until the removal of affected systems from agency control. In such cases, immediate actions will be required to ensure that the spillage is isolated and contained, and that unauthorized access is precluded based on risk management decisions and operational considerations related to the loss of information services. Preclusion of unauthorized access may include software overwriting of affected data sectors in the interest of meeting operational needs. When the media is released from agency control, sanitization is required.

3.3 Risk Assessment.

The Information Owner and the head or designee of the department/agency where the incident occurred shall collaborate in the performance of a risk assessment to determine mitigation procedures, with input from the responsible IRM and other appropriate parties. Such procedures apply to:

- Corrective actions including new procedures, technologies, security education, and other means to address causes (e.g., technical and procedural deficiencies, or incidents of negligence and deliberate disregard).
- Implementation of the mitigation procedures, while options should be taken to preserve continuity of operations.
- Ascertaining the degree of damage to national security, if the conclusion of the inquiry is a loss, possible compromise, or unauthorized disclosure of classified information.
- All hard copy material shall be marked with appropriate classification and storing it accordingly.
- All hard copy material shall be destroyed by approved classified destruction methods.

Phase 3 – Final Adjudication

Once the after-action report is created, OPS and OCIO notify the Administrator and Deputy Administrator when the investigation report is completed. Then, the OPS, in coordination with OCIO, will brief them on Corrective and Disciplinary actions taken or recommended.

The final AAR is created, in coordination with the SOC, by the Data Spillage Response Team. Once the entire process has been completed, the SOC retains the official copy of the AAR for future reporting and reference (within the AAR Repository).

Appendix A: Acronyms

AAR	After Action Report
ACES	Agency Consolidated End-User Services
CIO	Chief Information Officer
CIRT	Cyber Incident Response Team
CISO	Center Chief Information Security Officer
CNSI	Classified National Security Information
CNSS	Committee on National Security Systems
CSA	Cognizant Security Authority
EUSO	End User Service Office
HBK	Handbook
IMS	Incident Management System
IR	Incident Response
IRM	Incident Response Manager
ISSO	Information System Security Officer
IT	Information Technology
ITAR	International Traffic in Arms Regulations
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NPR	NASA Procedural Requirement
OCA	Original Classification Authority
OCIO	Office of the Chief Information Officer
ODV	Organizational Defined Value
OIG	Office of the Inspector General
OPS	The Office of Protective Services
OSM	Operation Security Manager
SOC	Security Operations Center
SP	Special Publication

Appendix B: Incident Action Examples

- The following incident action data should be captured as part of the data spillage process. At a minimum, they are:
- The actions that need to be taken following the spillage,
- The responsible individual for taking the actions (the Assignee), and
- The date the action was completed.

Sample action information for a spillage is captured below.

- **User**: Identify the user involved in the spillage.
- **Email**: Identify the user's email source.
- **Laptop/Desktop**: Identify the user's resources, including the asset number that may be impacted and/or involved in the spillage.
  - **Mobile Device(s)**: Identify whether the user read the information on their mobile device.
- **Back-up(s)**: Identify where the user's resource is backed up.
- **Printer(s)**: List out the related printers potentially impacted by the spillage.
- **Webmail**: Yes/No.
- **Action**: List the actions required as a result of the spillage.
- **Notes**: Include any relevant notes specific to each of the identified actions.
- **Assignee**: Identify the responsible organization/party for each of the identified actions.
- **Date Completed**: Document the date that each of the identified actions were completed.

Incident Action Example

User	Email	Laptop/Desktop	Mobile Device(s)	Back-up(s)	Printer(s)	Webmail
John Smith	NASA (NOMAD)	ACES issued, PC, Serial #	Not read	ACES	None	No
Jane Brown	NASA (NOMAD)	(ODIN) ACES issued, Mac, Serial #	Not read	ACES (1), Local (2)	None	No
Mike Williams	NASA (NOMAD)	Code 595 owned, Mac, Serial #	Not read	Local (1)	None	No
Ron White	NASA (NOMAD)	ACES issued, Mac, Serial #	Not read	ACES	Networked Printer	No

Actions

Action	Notes	Assignee	Date Completed
Sanitize devices for GSFC users	6 laptops, 1 printer, 2 external hard drives (local back-ups)	Center CISO	
Sanitize ACES back-ups	a. John, Jane, Mike, Ron; b. provide memo of actions taken back to Center OPS and Center CISO	SOC to provide direction to ACES contractor through EUSO	

Action	Notes	Assignee	Date Completed
Remove email chain from NOMAD servers, primary and back-up	Provide email chain report to Center OPS and Center CISO	SOC to provide direction to ACES contractor through EUSO	
Sanitize NOMAD servers, primary and back-up	Provide memo of actions taken back to Center OPS and Center CISO	SOC to provide direction to ACES contractor through EUSO	
Provide serial numbers: (a) primary and back-up NOMAD servers; (b) ACES back-up servers; (c) all devices involved in secondary incident	Provide serial numbers to Center OPS and Center CISO	SOC and EUSO	
Institute process for regular inventory of devices listed in (5), with final destruction upon end of life (prior to leaving Agency control)	Provide closure report to Center OPS and Center CISO	OCIO	
Final statement of record detailing technical sanitization activities conducted	GSFC CISO to GSFC OPS	Center CISO	
Final incident closure report	Can be provided to information owner	Center OPS	