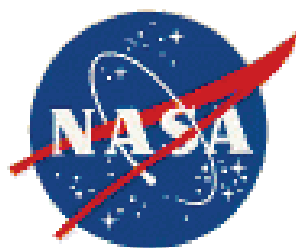




INFORMATION TECHNOLOGY SECURITY HANDBOOK

PRIVACY AWARENESS AND TRAINING

NOVEMBER 19, 2018



**COMPLIANCE WITH THE POLICIES, PROCEDURES, AND PROCESSES IN THIS
HANDBOOK IS MANDATORY**

Table of Contents

Table of Contents	2
Change History	3
1 Introduction	4
1.1 Purpose	5
1.2 Scope	5
1.3 Point(s) of Contact for this Handbook	5
1.4 Applicable Documents	5
2 Awareness and Training Process.....	6
2.1 Roles and Responsibilities	6
3 CPM Privacy Awareness and Training Activities	6
3.1 Roles and Responsibilities	7
Appendix A: Acronyms	8
Appendix B: Glossary	Error! Bookmark not defined.

Distribution:
NODIS

Associate Chief Information Officer for
Cybersecurity & Privacy

Change History

Version	Date	Change Description
1.0	09/07/2012	Initial draft
1.1	08/31/2015	Reviewed and signed by Associate CIO for IT Security
1.2	11/19/2018	Minor edits reviewed by Center Privacy Managers

1 Introduction

National Aeronautics and Space Administration (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*). *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*.

NPR 1382.1, NASA Privacy Procedural Requirements, designates this handbook as a guide for Chapter 7 of the NPR.

This handbook supports implementation of requirements in *NPD 1382.17, NASA Privacy Policy and NPR 1382.1, NASA Privacy Procedural Requirements*. It also augments NIST guidance with NASA-specific requirements, procedures and recommendations, where applicable. NASA-specific guidance does not negate NIST guidance, unless explicitly stated. The Agency's organizationally defined values are integrated into the control requirements within the Risk Information Security Compliance System (RISCS) system.

1.1 Purpose

In order to protect the privacy information entrusted to NASA, all NASA users of information and information systems must understand their privacy roles and responsibilities. To accomplish this end, the Senior Agency Official for Privacy (SAOP) provides the tools and training needed at the Agency level. Specifically, the NASA Chief Privacy Officer (CPO) develops the required privacy training and spearheads Agency-wide awareness efforts.

Ultimately the Center Privacy Managers (CPMs) are tasked with ensuring that NASA users at their respective Centers receive up-to-date and relevant privacy training. This handbook outlines the required CPM privacy efforts and establishes the basic requirements of the mandatory annual Center Breach Response Team (BRT) training and exercise.

1.2 Scope

This handbook supplements Chapter 7 of NPR 1382, *NASA Privacy Procedural Requirements*.

Compliance with this handbook is mandatory. Non-compliance or any unauthorized or improper use of NASA IT may result in the suspension or revocation of access to NASA IT, disciplinary action, as well as civil and criminal penalties.

If a handbook has or refers to an “expiration date” such date is tantamount to a “review date” for the handbook. This handbook and the policy/procedural guidance contained within remains in full force and effect until such time that the handbook is formally cancelled, rescinded or superseded by an updated document.

A documented rationale and/or justification shall accompany any non-concurrence, disapproval, denial, or request for deviation from the policy guidance or procedural requirements set forth in this handbook to support such decision. The documented rationale/justification shall be provided to the NASA Cybersecurity and Privacy Division (CSPD) and the point of contact for this handbook, in coordination with CPMs, to review and validate for the record.

1.3 Point(s) of Contact for this Handbook

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

- NASA Chief Privacy Officer

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 CPM, and directed to the attention of the point of contact for this particular handbook to address and resolve.

1.4 Applicable Documents

Office of Management and Budget (OMB)

- *OMB Circular A-130, Managing Information as a Strategic Resource*

- *OMB Memorandum M-17-12, Preparing for and Responding to a Breach of Personally Identifiable Information*

National Aeronautics and Space Administration (NASA)

- *NPD 1382.17, NASA Privacy Policy*
- *NPR 1382.1, NASA Privacy Procedural Requirements*
- *ITS-HBK-1382.09-01, Privacy Rules of Behavior*

2 Awareness and Training Process

The NASA Chief Privacy Officer has oversight over the content of all NASA privacy training materials intended for Agency-wide availability. Local or Center developed privacy training shall be, in all respects, commensurate with Agency training (with the exception of any additional materials necessary to meet local Center requirements). The CPM is responsible for Center level privacy training requirements and materials and ensures that training materials provided by the NASA CPO are incorporated, at a minimum, in a way which ensures no conflicts exist.

2.1 Roles and Responsibilities

Agency-Wide

- *The NASA Chief Privacy Officer (CPO) shall:*
 - Develop the NASA privacy training materials and provide content to the Information Technology Security Awareness and Training Center (ITSATC).
 - Provide the CPMs with the NASA privacy training materials for review and comment.
 - Incorporate CPM comments to NASA privacy training materials, as appropriate.
- *The ITSATC shall:*
 - Work with the NASA Privacy Programs Manager to ensure that the NASA privacy training materials are appropriately communicated to the NASA users.
 - Track privacy training statistics and provide them to the NASA Chief Privacy Officer in Quarter 4 of the Fiscal Year, and as requested.

Center Level

- *Center Privacy Manager (CPM) shall:*
 - Review NASA privacy training materials and respond with comments.
 - Ensure that the NASA users at the Center receive the required privacy training on an annual basis (per OMB requirements).
 - Provide privacy awareness materials to NASA users at the Center.

3 CPM Privacy Awareness and Training Activities

To increase NASA user awareness, the CPM shall implement awareness and training opportunities at the Center level to ensure heightened awareness of privacy requirements year round.

3.1 Roles and Responsibilities

Agency-Wide

- *The NASA Chief Privacy Officer (CPO) shall:*
 - Provide guidance to the CPMs as they implement awareness and training at the Centers.

Center Level

- *Center Privacy Manager (CPM) shall:*
 - Ensure that NASA users at the Center are provided with awareness materials on an annual basis, at a minimum.
 - Provide annual privacy BRT training to all designated Center BRT members by Quarter 3 of the fiscal year.
 - Privacy BRT Training shall include:
 - An outline of BRT member roles and responsibilities.
 - An overview of the privacy BRT process.
 - A tabletop exercise – a scenario that allows the BRT members to exercise the complete process and their roles within the process.
 - Upload any Center awareness and training materials to the Privacy Management SharePoint site in the Center's Training folder.
- *The Center BRT members shall:*
 - Attend annual BRT member training.
- *The NASA user shall:*
 - Participate in mandatory privacy training prior to gaining access to NASA information and information systems, and yearly thereafter.

Appendix A: Acronyms

BRT	Breach Response Team
CPM	Center Privacy Manager
CPO	Chief Privacy Officer
CSPD	Cybersecurity and Privacy Division
FIPS	Federal Information Processing Standards
ISO	Information System Owner
ITSATC	Information Technology Security Awareness and Training Center
ITS-HBK	Information Technology Security Handbook
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
OMB	Office of Management and Budget
RISCS	Risk Information Security Compliance System
SAOP	Senior Agency Official for Privacy
SP	Special Publication