



NASA TECHNICAL HANDBOOK

National Aeronautics and Space Administration

ITS-HBK-2810.12-02 v2024-02

Published: 2024-02-23

**Physical and Environmental Protection
TECHNICAL HANDBOOK**

TABLE OF CONTENTS

Document Properties	4
Document History Log	4
Approval	4
1. Introduction	5
1.1. Purpose	5
1.2. Scope	5
1.3. Point of Contact(s)	6
1.4. Applicability	6
1.5. Applicable Documents	6
1.5.1. Federal Information Processing Standards (FIPS)	6
1.5.2. National Institute of Standards and Technology (NIST)	6
1.5.3. National Aeronautics and Space Administration (NASA)	6
1.5.4. Cancellations, Updates, Consolidations	6
2. Security Controls, Roles and Responsibilities	7
2.1. Physical Access Authorizations (PE-2)	7
2.1.1. Office of Protective Services (OPS)	7
2.1.2. Information System Owner (ISO)	7
2.2. Physical Access Control (PE-3)	7
2.2.1. Information System Owner (ISO)	7
2.2.2. Office of Protective Services (OPS)	7
2.3. Physical Access Control: System Access (PE-3(1))	8
2.3.1. Office of Protective Services (OPS)	8
2.4. Access Control for Transmission (PE-4)	8
2.4.1. Office of Protective Services (OPS)	8
2.5. Access Control for Output Devices (PE-5)	8
2.5.1. Office of Protective Services (OPS)	8
2.5.2. Information System Owner (ISO)	8
2.6. Monitoring Physical Access (PE-6)	8
2.6.1. Office of Protective Services (OPS)	8
2.6.2. Information System Owner (ISO)	9
2.7. Monitoring Physical Access: Intrusion Alarms/Surveillance Equipment (PE-6(1))	9
2.7.1. Office of Protective Services (OPS)	9
2.8. Monitoring Physical Access: Monitoring Physical Access to Information Systems (PE-6(4))	9
2.8.1. Office of Protective Services (OPS)	9
2.9. Visitor Control (PE-7)	9
2.10. Visitor Access Records (PE-8)	9
2.10.1. Information System Owner (ISO)	9
2.11. Visitor Access Records: Automated Records Maintenance/Review (PE-8(1))	10
2.11.1. Office of Protective Services (OPS)	10
2.12. Power Equipment and Power Cabling (PE-9)	10
2.12.1. Information System Owner (ISO)	10
2.13. Emergency Shutoff (PE-10)	10
2.13.1. Office of Strategic Infrastructure (OSI)	10
2.14. Emergency Power (PE-11)	10
2.14.1. Information System Owner (ISO)	10

2.15. Emergency Lighting (PE-12)	10
2.15.1. Office of Strategic Infrastructure (OSI)	10
2.16. Fire Protection (PE-13)	11
2.16.1. Office of Strategic Infrastructure (OSI)	11
2.17. Environmental Controls (PE-14)	11
2.17.1. Office of Strategic Infrastructure (OSI)	11
2.18. Water Damage Protection (PE-15)	11
2.18.1. Office of Strategic Infrastructure (OSI)	11
2.19. Water Damage Protection: Automation Support (PE-15(1))	11
2.19.1. Office of Strategic Infrastructure (OSI)	11
2.20. Delivery and Removal (PE-16)	11
2.20.1. Information System Owner (ISO)	11
2.21. Alternate Work Site (PE-17)	12
2.21.1. Center Chief Information Security Officer (Center CISO)	12
2.22. Location Information System Components (PE-18)	12
2.22.1. Office of Strategic Infrastructure (OSI)	12
Appendix A: Acronyms	12

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.
1.3	2014-12-15	Extended for revision of Rev 4 controls and updates
1.4	2015-02-23	Revised Section 10
1.5	2017-02-14	Extended for updates
1.6	2017-04-12	Updated to reflect new tools and maintain consistency with referenced documents/standards
1.7	2018-08-01	Updated for consistency with new Handbook format
1.8	2021-09-30	Updated to reflect NIST SP 800-53 Rev. 5
1.9	2023-01-31	Annual update.
v2023-06	2023-06-16	Updated to new format
v2024-02	2024-02-23	Annual update

Approval



Associate Chief Information Officer for
Cybersecurity & Privacy

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 (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 Rev. 5, 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). NASA Policy Directive (NPD) 2810.1, NASA Information Security Policy, NASA Procedural Requirements (NPR) 2810.1, Security of Information Technology and Information Systems, and the collection of 2810 Information Technology Handbooks (ITS HBK) satisfy the policy and procedure controls of NIST SP 800-53 Rev.5.

[NPR 2810.1](#) designates this Handbook as a guide of NASA's Physical and Environmental Protection (PE) information security controls, and the content of this document, in conjunction with NPD/R 2810.1, defines NASA policy and procedures to address [PE-1](#).

This Handbook supports implementation of requirements in [NPR 2810.1](#) and [NPD 2810.1](#). 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 RSAARCHER in the Risk Information Security Compliance System (RISCS).

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.

1.1. Purpose

The purpose of this Handbook is to provide consistent controls for protecting and maintaining NASA's physical facilities.

1.2. Scope

This Handbook applies to protections for all NASA-owned and NASA-operated systems. NASA contractor systems shall also implement the controls required by this Handbook (or more stringent ones).

Although NASA handbooks may contain "shall" (requirements) statements, they are not intended to be requirements documents. However, pursuant to NPR 1400.IK, portions of NASA handbooks containing procedural, or process guidance may be cited in contract, program, and other Agency documents, and may become requirements when a NASA directive specifies their use by citing the document title, revision letter/number, and date; or, when a NASA manager with authority over a NASA program, project, or other activity, identifies it as a requirement.

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 Center Chief Information Security Officers (CISO), to review and validate for the record.

1.3. Point of Contact(s)

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

- hg-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 particular 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, 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

1.5.1. 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*](#)

1.5.2. National Institute of Standards and Technology (NIST)

- [NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*](#)
- [NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*](#)

1.5.3. National Aeronautics and Space Administration (NASA)

- [NPD 2810.1, *NASA Information Security Policy*](#)
- [NPR 1600.1, *NASA Security Program Procedural Requirements*](#)
- [NPR 1620.3, *Physical Security Requirements for NASA Facilities and Property*](#)
- [NPR 2810.1, *Security of Information and Information Systems*](#)
- [ITS-HBK-2810.10-02, *Maintenance*](#)
- [ITS-HBK-2810.11-02, *Media Protection and Sanitization*](#)

1.5.4. Cancellations, Updates, Consolidations

- ITS-HBK 2810.12-01A: Physical and Environmental Protection

2. SECURITY CONTROLS, ROLES AND RESPONSIBILITIES

2.1. Physical Access Authorizations (PE-2)

2.1.1. Office of Protective Services (OPS)

The Office of Protective Services (OPS):

- Issues authorization credentials for facility access.
- Reviews the access list detailing authorized facility access by individuals two times per year.
- Removes individuals from the facility access list when access is no longer required.

2.1.2. Information System Owner (ISO)

The ISO:

- Establishes minimum requirements for any individual to obtain credentials for physical access to the information system in a manner consistent with organizationally defined values.
- Develops, approves, and maintains a list of individuals with authorized access to the facility where the information system resides.
- Ensures that personnel no longer requiring access to the facility are removed from access lists.

2.2. Physical Access Control (PE-3)

2.2.1. Information System Owner (ISO)

The ISO:

- Establishes additional restrictions (beyond whatever is standard at their Center) for physical access to their system, as necessary.

2.2.2. Office of Protective Services (OPS)

The OPS shall:

- Enforces physical access authorizations at entry/exit points used for non-emergency personnel access and as further defined by the ISO by:
 - Verifying individual access authorizations before granting access to the facility.
 - Controlling ingress/egress to the facility using physical access control systems, devices, and/or guards in a manner consistent with organizationally defined values.
- Maintains physical access audit logs for entry/exit points in accordance with NPR 1600.1.
- Provides physical access controls in accordance with NPR 1600.1 to control access to areas within the facility officially designated as publicly accessible.

- Escorts visitors and monitors visitor activity when in proximity to information system components.
- Secures keys, combinations, and other physical access devices.
- Inventories keys and combinations every two years (Key Accountability).
- Changes combinations and keys:
 - Keys - one to three years
 - Combinations - two years
 - Whenever keys are lost, combinations are compromised, or individuals are transferred or terminated.

2.3. Physical Access Control: System Access (PE-3(1))

2.3.1. Office of Protective Services (OPS)

The OPS:

- Enforces physical access authorizations to the information system in addition to the physical access controls for the facility at all spaces with a concentration of information system components (e.g., servers, hubs, routers).

2.4. Access Control for Transmission (PE-4)

2.4.1. Office of Protective Services (OPS)

The OPS:

- Controls physical access to information system distribution and transmission line termination points within organizational facilities using the requirements as specified in NPR 1620.3.

2.5. Access Control for Output Devices (PE-5)

2.5.1. Office of Protective Services (OPS)

The OPS:

- Controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

2.5.2. Information System Owner (ISO)

The ISO:

- Where possible, places output devices for the information in secured areas of the facility and/or locations that can be monitored by organizational personnel.

2.6. Monitoring Physical Access (PE-6)

2.6.1. Office of Protective Services (OPS)

The OPS:

- Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents.

2.6.2. Information System Owner (ISO)

The ISO:

- Reviews information system physical access logs for suspicious physical activities 1/month and upon occurrence of indication of compromise or misuse of resources.
- Coordinates results of the reviews and investigation of suspicious activity with the
- Center Chief Information Security Officer (CISO), Information System Security Officer (ISSO), Center Chief of Security (CCS), OPS, and the Security Operations Center (SOC).

2.7. Monitoring Physical Access: Intrusion Alarms/Surveillance Equipment ([PE-6\(1\)](#))

2.7.1. Office of Protective Services (OPS)

The OPS:

- Monitors physical intrusion alarms and surveillance equipment.

2.8. Monitoring Physical Access: Monitoring Physical Access to Information Systems ([PE-6\(4\)](#))

2.8.1. Office of Protective Services (OPS)

The OPS:

- Monitors physical access to the information system in addition to the physical access monitoring of the facility as all spaces with a concentration of information system components (e.g., servers, hubs, routers, etc.).

2.9. Visitor Control ([PE-7](#))

This control has been withdrawn. It is now incorporated into [PE-2](#) and [PE-3](#).

2.10. Visitor Access Records ([PE-8](#))

2.10.1. Information System Owner (ISO)

The ISO:

- Ensures visitor access records to non-public areas of facilities where information systems reside are maintained for at least 6 months, in coordination with the Center CISO, ISSO, CCS, and OPS.
 - Visitor access records should contain the name and organization of the visitor, signature of the visitor, forms of identification provided, date of access, time of entry, time of departure, purpose of visit, and the name/organization of the person visited.
- Ensures access records are reviewed, in coordination with the Center CISO, ISSO, CCS, and OPS, 1/month.

- Report anomalies in visitor access records in accordance with organizational-defined values.

2.11. Visitor Access Records: Automated Records Maintenance/Review (PE-8(1))

2.11.1. Office of Protective Services (OPS)

OPS:

- Employs automated mechanisms to facilitate the maintenance and review of visitor access records.

2.12. Power Equipment and Power Cabling (PE-9)

2.12.1. Information System Owner (ISO)

The ISO:

- Coordinates with Center facilities personnel to protect power equipment and power cabling for the information system from damage and destruction.

2.13. Emergency Shutoff (PE-10)

2.13.1. Office of Strategic Infrastructure (OSI)

The Office of Strategic Infrastructure (OSI):

- Ensures facilities, such as data centers, have emergency shutoff capabilities compliant with [NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations](#) that:
 - Are consistent with organizational-defined values;
 - Allow the power shutoff to concentrations of information systems or components without requiring individuals to approach the equipment;
 - Have emergency switches or devices in the facility at or near the exit door of the facility and/or room of the facility; and
 - Are located and protected to prevent shutoff from accidental or unauthorized activation.

2.14. Emergency Power (PE-11)

2.14.1. Information System Owner (ISO)

The ISO:

- Coordinates with Center facilities personnel to provision a short-term uninterruptible power supply to facilitate an orderly shutdown of their information system in the event of a primary power source loss.

2.15. Emergency Lighting (PE-12)

2.15.1. Office of Strategic Infrastructure (OSI)

The OSI:

- Ensures all facilities in which information systems reside have operational emergency lighting that activates in the event of power outage/disruption that covers emergency exits and evacuation routes within the facility, in accordance with [NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*](#).

2.16. Fire Protection (PE-13)

2.16.1. Office of Strategic Infrastructure (OSI)

The OSI:

- Ensure all facilities in which information systems reside employ and maintain fire suppression and detection devices/systems that are supported by an independent energy source.

2.17. Environmental Controls (PE-14)

2.17.1. Office of Strategic Infrastructure (OSI)

The OSI:

- Maintains temperature and humidity levels within the facility where information systems reside at:
 - Temperature: 65 to 75 degrees Fahrenheit, and
 - Humidity 50% (plus or minus 15%).
- Monitors temperature and humidity levels continuously.

2.18. Water Damage Protection (PE-15)

2.18.1. Office of Strategic Infrastructure (OSI)

The OSI:

- Coordinates with Center facilities personnel to protect information systems from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

2.19. Water Damage Protection: Automation Support (PE-15(1))

2.19.1. Office of Strategic Infrastructure (OSI)

The OSI:

- Employs automated mechanisms to detect the presence of water in the vicinity of information systems and alerts Center emergency responders/Center operations.

2.20. Delivery and Removal (PE-16)

2.20.1. Information System Owner (ISO)

The ISO:

- Authorizes and controls all information system-related items including hardware and software components and system software media entering and exiting the facility and maintain a record of those items in accordance with organizationally defined values, ITS-HBK-2810.10-02B, and ITS-HBK 2810.11.

2.21. Alternate Work Site (PE-17)

2.21.1. Center Chief Information Security Officer (Center CISO)

The Center CISO:

- Determines and documents alternate work sites in accordance with organizational-defined values.
- Employs at a minimum the following controls as described in the System Security Plan (SSP) approved under the current Authorization to Operate (ATO):
 - All Management Controls;
 - Media Protection (MP) controls;
 - All technical controls related to Access Control and Identification & Authentication; and
 - All Privacy controls at alternate work sites.
- Assesses as feasible the effectiveness of security controls at alternate work sites.
- Provides a means for employees to communicate with information security personnel in case of security incidents or problems.

2.22. Location Information System Components (PE-18)

2.22.1. Office of Strategic Infrastructure (OSI)

The OSI:

- Positions information system components within the facility to minimize potential damage from flooding or water leaks, wind damage to the facility/building, inadvertent activation of fire suppression systems, and/or other hazards as defined by the Center or ISO and to minimize the opportunity for unauthorized access.

APPENDIX A: ACRONYMS

ATO	Authorization to Operate
CCS	Center Chief of Security
CIO	Chief Information Officer
CISO	[Center] Chief Information Security Officer
CSPD	Cybersecurity and Privacy Division
FFRDC	Federally Funded Research and Development Center
FIPS	Federal Information Processing Standards

HBK	Handbook
ISO	Information System Owner
ISSO	Information System Security Officer
IT	Information Technology
ITS	Information Technology Security
MP	Media Protection .
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
OPS	Office of Protective Services
OSI	Office of Strategic Infrastructure
PE	Physical and Environmental Security
soc	Security Operations Center
SP	Special Publication
SSP	System Security Plan