



NASA TECHNICAL HANDBOOK

National Aeronautics and Space Administration

ITS-HBK-2810.15-01 v2024-02

Published: 2024-02-23

**Access Control
TECHNICAL HANDBOOK**

TABLE OF CONTENTS

Document Properties	4
Document History Log	4
Approval	4
1. Introduction	5
1.1. Scope	5
1.2. Point of Contact(s)	5
1.3. Applicability	5
1.4. Applicable Documents	5
1.4.1. Federal Information Processing Standards (FIPS)	5
1.4.2. National Institute of Standards and Technology (NIST)	6
1.4.3. National Aeronautics and Space Administration (NASA)	6
2. Account Management (AC-2)	6
2.1. Roles and Responsibilities	6
2.1.1. Center Chief Information Officer (CIO)	6
2.1.2. Information System Owner (ISO)	6
2.1.3. NAMS Project Manager	7
3. Access Enforcement (AC-3)	7
4. Information Flow Enforcement (AC-4)	7
5. Separation of Duties (AC-5)	7
6. Least Privilege (AC-6)	7
6.1. Roles and Responsibilities	8
6.1.1. Information System Owner (ISO)	8
7. Unsuccessful Login Attempts (AC-7)	8
7.1. Roles and Responsibilities	8
7.1.1. Information System Owner (ISO)	8
8. System Use Notification (AC-8)	8
8.1. Roles and Responsibilities	8
8.1.1. Information System Owner (ISO)	8
8.1.2. NASA User	9
9. Concurrent Session Control (AC-10)	9
9.1. Roles and Responsibilities	9
9.1.1. Information System Owner (ISO)	9
10. Session Lock (AC-11)	9
10.1. Roles and Responsibilities	9
10.1.1. Information System Owner (ISO)	9
11. Permitted Actions without Identification or Authentication (AC-14)	9
12. Remote Access (AC-17)	9
12.1. Roles and Responsibilities	9
12.1.1. Information System Owner (ISO)	9
12.1.2. NASA User	10
13. Wireless Access (AC-18)	10
13.1. Roles and Responsibilities	10
13.1.1. Center Chief Information Security Officer (Center CISO)	10
13.1.2. Information System Owner (ISO)	10
14. Access Control for Mobile Devices (AC-19)	11

14.1. Roles and Responsibilities	11
14.1.1. Information System Owner (ISO)	11
15. Publicly Accessible Content (AC-22)	11
15.1. Roles and Responsibilities	11
15.1.1. Information System Owner (ISO)	11
16. Elevated Privileges	11
16.1. Roles and Responsibilities	11
16.1.1. Center Chief Information Officer (Center CIO)	11
16.1.2. Information System Owner (ISO)	12
16.1.3. Information System Security Officer (ISSO)	12
16.1.4. NASA User	12
16.1.5. System Administrator	13
Appendix A: Acronyms	14

DOCUMENT PROPERTIES

Document History Log

Document Version	Published Date	Description
1.0	2011-05-02	Initial Draft
1.1	2011-12-21	Incorporated items from the NITR 2810-14A that were not included in the NPR 2810.1 update
A	2012-09-04	Organization-defined Values Description AC-11 clerical update to include missing word “example.”
1.2	2014-12-04	One-year extension due to revisions
1.3	2015-09-30	Extended due to revisions
1.4	2017-04-17	Updated to reflect new tools and maintain consistency with referenced documents/standards
1.5	2019-11-25	Reformatted and expiration date removed
1.6	2021-09-30	Updated with NIST 800-53 Rev.5 provisions.
1.7	2023-01-31	Annual update.
v2023-06	2023-06-16	Updated to new format
v2024-02	2024-02-23	Annual update. Hyperlinks fixed, bullets properly indented.

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 ([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*](#)). 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 Access Control (AC) information security controls. The content of this document, in conjunction with NPD/R 2810.1, defines NASA policy and procedures to address [AC-1](#)

1.1. Scope

The Access Control security control family relates to the ability of NASA to permit or deny access to computer systems, system locations and system information based on a user's need to know. The control family encompasses the management of unique account identifiers (IDs), passwords, physical access, badges and tokens, and user permissions to ensure the proper level of system access.

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

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.

1.3. Applicability

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. The Agency's organization-defined values are integrated into the control requirements within RSA ARCHER in the Risk Information Security Compliance System (RISCS) system. 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.

1.4. 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 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- NIST SP 800-46, *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security*
- NIST SP 800-53, *Security and Privacy Controls for Information Systems and Organizations*
- NIST SP 800-63-3, *Digital Identity Guidelines*
- NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*
- NIST SP 800-121, *Guide to Bluetooth Security*

1.4.3. National Aeronautics and Space Administration (NASA)

- NPD 2540.1, *Acceptable Use of Government Furnished Information Technology Equipment, Services and Resources*
- NPD 2810.1, *NASA Information Security Policy*
- NPR 2810.1, *Security of Information and Information Systems*
- NPR 2841.1, *Identity, Credential, and Access Management*
- NASA EA-STD-0001 Standard for Integrating Applications into the NASA Access Management, Authentication, and Authorizations Infrastructure
- ITS-HBK-2810.11-02, *Media Protection and Sanitization*
- ITS-HBK-2810.15-02, *Access Control: Managed Elevated Privileges (EP)*
- Homeland Security Presidential Directive 12 (HSPD-12), *Policy for a Common Identification Standard for Federal Employees and Contractors*

2. ACCOUNT MANAGEMENT (AC-2)

2.1. Roles and Responsibilities

2.1.1. Center Chief Information Officer (CIO)

The Center Chief Information Officer (CIO) shall:

- Review and approve waivers for granting elevated privileges to users without the requisite training in accordance with ITS-HBK-2810.15-02.
- The Center CIO may delegate the responsibility for the review and approval of waivers to the Center Information Security Official (CISO) or other NASA staff, but not to the account issuer.
- Waivers shall not exceed 90 days and should include justification for its provisions.

2.1.2. Information System Owner (ISO)

The Information System Owner (ISO) shall:

- Identify account types (e.g., security roles, user privilege groups) for NASA users of their information systems in the NASA Access Management System (NAMS).
- Identify conditions necessary to be granted identified account types, in NAMS.

- Require appropriate criteria for approving requests to establish accounts (e.g., training requirements) in NAMS.
- Monitor any changes to privileged roles or attributes and revoke access when privileged role or attribute assignments are no longer appropriate.
- Authorize and monitor the use of guest/anonymous/temporary/privileged accounts.
 - Guest and anonymous accounts should only be used when the content and services being accessed are public in nature.
 - Temporary accounts should be provisioned through NAMS.
- Ensure a timely deactivation of accounts which are no longer needed, and accounts of terminated or transferred users in accordance with organization-defined values.
- Have the authority to approve elevated user privileges on their information system in an emergency situation, consistent with guidance in ITS-HBK-2810.15-02.
 - Emergency elevated user privileges shall be limited to the minimum duration needed to deal with the particular emergency.

2.1.3. NAMS Project Manager

The NAMS Project Manager shall:

- Establish procedures for the authorization, establishment, activation, modification, disabling, and removal of accounts in NAMS.
- Ensure the capability to automatically disable temporary, emergency, and inactive accounts.
- Notify the Security Operations Center (SOC) or appropriate organization (e.g., Center-specific IT Security office, incident response team, or help desk) of any NAMS workflows used to manage the authorization of accounts with elevated privileges.
- Ensure that NAMS workflows used to manage elevated privileges meet requirements described in ITS-HBK-2810.15-02.

3. ACCESS ENFORCEMENT (AC-3)

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.

4. INFORMATION FLOW ENFORCEMENT (AC-4)

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.

5. SEPARATION OF DUTIES (AC-5)

- 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.
- Administrator accounts must not be allowed to also administer audit functions in NASA systems. This separation should be managed through the use of different accounts with different system access authorizations.

6. LEAST PRIVILEGE (AC-6)

6.1. Roles and Responsibilities

6.1.1. Information System Owner (ISO)

The ISO shall:

- Ensure users of information systems are assigned access authorizations only to the degree necessary to carry out their responsibilities.
- Approve the provision of administrator access and elevate privileges for their information systems in accordance with ITS-HBK-2810.15-02.

7. UNSUCCESSFUL LOGIN ATTEMPTS (AC-7)

7.1. Roles and Responsibilities

7.1.1. Information System Owner (ISO)

The ISO shall:

- Ensure the capability to enforce appropriate system access limitations as a result of unsuccessful login attempts in a manner consistent with organization-defined values.
- Enable automatic account lockout according to organizational-defined values for unsuccessful login attempts unless this automation creates mission impacts.

8. SYSTEM USE NOTIFICATION (AC-8)

8.1. Roles and Responsibilities

8.1.1. Information System Owner (ISO)

The ISO shall:

- Ensure the display of the System Use Notification, as defined by [NPR 2810.1](#), on any information system which includes an interactive login interface.
 - An information system shall maintain display of system use notifications and prevents further access, until explicit action is taken by the user to accept all terms and conditions.
 - This applies to all computers and applications that are owned or operated on behalf of NASA and require user authentication for access.
- Ensure that the appropriate warning banner, as defined by [NPR 2810.1](#), is displayed on NASA resources or information systems utilizing NASA networks until explicit action is taken by a user to accept all terms and conditions. This includes any information system components:
 - On a network whose addresses are assigned to NASA;
 - That processes NASA data (public or non-public);
 - That is actively or potentially managed by or on behalf of NASA; or
 - That is actively or potentially monitored by or on behalf of NASA.

8.1.2. NASA User

The NASA User shall:

- Agree to the appropriate use policy statement based on [NPD 2540.1, *Acceptable Use of Government Furnished Information Technology Equipment, Services and Resources*](#) and approved by the NASA General Counsel, prior to being granted access to any NASA information system.

9. CONCURRENT SESSION CONTROL (AC-10)

9.1. Roles and Responsibilities

9.1.1. Information System Owner (ISO)

The ISO shall:

- Ensure the capability to limit the number of concurrent sessions on an information system in a manner consistent with organization-defined values.

10. SESSION LOCK (AC-11)

10.1. Roles and Responsibilities

10.1.1. Information System Owner (ISO)

The ISO shall:

- Ensure the capability to lock a user session following a determined length of inactivity in a manner consistent with organization-defined values.
- Ensure system utilizes a publicly viewable image to conceal controlled unclassified information from public display while the system is locked.

11. PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION (AC-14)

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.

12. REMOTE ACCESS (AC-17)

12.1. Roles and Responsibilities

12.1.1. Information System Owner (ISO)

The ISO shall:

- Ensure only devices that are authorized and approved for remote access to the information system to which they

are connecting are granted remote access in a manner consistent with organization-defined values.

- National Security or classified information shall not be processed, stored, or transmitted on personally-owned or third-party devices at any time.
- When employing multifactor authentication for remote access to information systems, ensure that the authentication mechanism is [SP 800-63-3](#) Level 4 compliant using the PIV card.
 - 2-factor identification using the PIV card shall be required for remote access to non-privileged accounts.
- Ensure that remote access is routed through NASA network access control points.

12.1.2. NASA User

The NASA User shall:

- Use only NASA authorized and approved devices for remote access to NASA non-public information systems.
- If teleworking, have a telework agreement in place.
- Take every reasonable effort to ensure the confidentiality, integrity, and availability of information and information systems used remotely (e.g., not leaving laptops and other devices unattended or in public plain view).
- Understand their responsibilities for protecting Personally Identifiable Information (PII) data, and the consequences for mishandling PII.

13. WIRELESS ACCESS ([AC-18](#))

13.1. Roles and Responsibilities

13.1.1. Center Chief Information Security Officer (Center CISO)

The Center CISO shall:

- Provide the capability to scan for unauthorized wireless systems.
- Ensure unauthorized wireless systems are disabled and reported immediately to the SOC or appropriate organization (e.g., Center-specific IT Security office, incident response team, or help desk).
- Ensure the scanning of information systems for unauthorized wireless access points or otherwise posing risk to NASA information systems, in a manner consistent with organization-defined values.

13.1.2. Information System Owner (ISO)

The ISO shall:

- Ensure that only wireless systems that meet approved authentication protocols are used for Local Area Networks (LAN) or as access points to NASA information systems.
- Ensure that user level authentication and encryption is utilized to protect wireless access to the system.
- Ensure that embedded wireless networking capabilities within system components are disabled prior to issuance or deployment when not intended for use.
- Ensure a risk analysis with consideration to the guidelines of NIST SP 800-121 Revision 1 is conducted prior to the use of Bluetooth technologies for NASA devices.

14. ACCESS CONTROL FOR MOBILE DEVICES (AC-19)

14.1. Roles and Responsibilities

14.1.1. Information System Owner (ISO)

The ISO shall:

- Ensure that only NASA-approved and authorized mobile devices are used to access non-public NASA information systems.
 - Approved and authorized mobile devices are those devices that are purchased and owned or contracted for use by NASA government or contract employees (e.g., Workspace Collaborative System (WCS), NASA IT Infrastructure Improvement Program (I3P) devices).
- Ensure that mobile devices carried on travel to locations where there is concern for the loss or compromise of NASA sensitive information are examined upon return for physical tampering.
- Ensure that all disk media for mobile devices carried on travel to locations deemed to be of significant risk are sanitized in accordance with [ITS-HBK-2810.11-02, Media Protection and Sanitization](#) and re-imaged, if required, upon return.

15. PUBLICLY ACCESSIBLE CONTENT (AC-22)

15.1. Roles and Responsibilities

15.1.1. Information System Owner (ISO)

The ISO shall:

- Review new content on publicly accessible information systems and monitor for any information which may not be approved for public release in a manner consistent with organization-defined values.
- Remove immediately any information deemed to be not approved for public release from any publicly accessible information system.

16. ELEVATED PRIVILEGES

More detailed information on the requirements for requesting, implementing, and managing elevated privileges may be found in ITS-HBK-2810.15-02, Managed Elevated Privileges (EP) Implementation Handbook.

16.1. Roles and Responsibilities

16.1.1. Center Chief Information Officer (Center CIO)

The Center CIO shall:

- Review and approve/deny all requests for elevated user privileges.
- Maintain authority to approve requests for elevated privileges on all NASA information systems which reside at

their Center, or whose system security plans are managed at their Center.

- Verify that qualification requirements (e.g., training) have been met before approving a request for elevated user privileges or waive these requirements on a case-by-case basis in accordance with ITS-HBK-2810.15-02.
- 16.2.1.4
- Maintain the ability to revoke elevated privileges.

16.1.2. Information System Owner (ISO)

The ISO shall:

- Ensure that all information system users with elevated privileges have been authorized to hold those privileges.
- Ensure that elevated privileges are granted only to those users who are qualified to access the information system.
- Ensure that elevated privileges are used only for the purposes for which they were granted.
- Maintain the ability to revoke elevate privileges.
- Ensure that appropriate elevated privilege documentation is maintained:
 - All authorizations for elevated privileges shall be documented and managed in the NASA Account Management System (NAMS).
 - Each SSP shall reference the NAMS workflow being used to document and manage elevated user privileges for the information system

16.1.3. Information System Security Officer (ISSO)

The Information System Security Officer (ISSO) shall:

- Periodically review and validate that only authorized accounts have elevated privileges.
- Ensure that elevated privileges are used only in a form consistent with the usage justification.
- Maintain the ability to revoke elevated privileges.

16.1.4. NASA User

The NASA User shall:

- Meet the following requirements in order to qualify for elevated privileges:
 - Renew all applicable SATERN training once a year and/or maintain all relevant industry certifications.
 - Demonstrate knowledge of the following topics: (Note: The following may be demonstrated through the completion of SATERN certification for elevated privileges)
 - The risks of accessing a computer with elevated privileges, to the information stored on the computer, to the computer itself, and to other NASA devices in the same environment.
 - Best practices and precautions to be used when accessing an information system with elevated privileges.
 - User responsibilities associated with accessing a NASA information system with elevated privileges.
 - Be responsible for the consequences of his/her actions performed on a NASA information system during the user's access with elevated privileges in accordance with the User Acknowledgement Statement agreed to in the NAMS request workflow.
- If granted elevated privileges for a period exceeding 30 days (for one authorization, or cumulatively for multiple

authorizations within the period of one year), in addition to the qualification requirements in section 16.2.4.1, demonstrate knowledge of the following topics: (Note: The following may be demonstrated through the completion of SATERN "IT Security for Systems Administrators, Beginner Level" course, or by completing commensurate certifications and/or classroom or on-on-one training).

- Incident Response (including identifying potential incidents; knowing how, when, and to whom to report potential or actual incidents; knowing how to recover from an incident).
- Security Program Management Compliance (including understanding the purpose of and elements of the Information Security Program; applying Information Security Program elements to the information system; identifying areas of weakness in the Information Security Program).
 - Security components of each phase in the System Development Life Cycle (SDLC), including:
 - Knowing which security controls to implement and how;
 - Recognizing weakness in a security control;
 - Recognizing if the security controls are not implemented according to the implementation plan;
 - Understanding security ramifications of changes to a system;
 - Knowing how to modify security controls to accommodate changes in operations;
 - Understanding that each system impacts the security of other systems to which is being connected;
 - Knowing the information security responsibilities of users of the information system;
 - Monitoring information systems to identify potential information security incidents;
 - Understanding and meeting all data retention and disposal requirements; etc.).
- Use elevated privileges only for the purposes for which they were granted.

16.1.5. System Administrator

The System Administrator shall:

- Meet all requirements of a NASA User in seeking elevated privileges.
- Demonstrate knowledge of the following: (Note: The following may be demonstrated through the completion of SATERN "IT Security for Systems Administrators, Intermediate Level or other approved certification/training):
 - Incident Response (including making decisions on whether policy has been breached and if further action is needed).
 - Security Program Management Compliance (including interpreting compliance with NASA's IT Security Program and analyzing patterns of non-compliance).
 - Security components of each phase in the SDLC, including:
 - Analyzing system performance and approving system configuration and functionality;
 - Assessing, understanding, and interpreting performance of security controls and their effect on changes on security vulnerabilities;
 - Identifying new vulnerabilities; assessing security controls' ability to correct new vulnerabilities, and applying new or modified controls;
 - Knowing how to accommodate operational changes and maintain an acceptable level of risk;
 - Understanding procedures to follow for actual security incidents;
 - Knowing how to apply NASA security policy to the disposal of information and systems and how to decide on the best way to dispose of assets no longer in use; and
 - Knowing how to conduct proper archiving, sanitizing, or disposition of all hardware, software, data, and

facility resources; etc.

APPENDIX A: ACRONYMS

CIO	Chief Information Office
CISO	Center Chief Information Security Officer
EP	Elevated Privileges
FIPS	Federal Information Processing Standards
HBK	Handbook
IMS	Incident Management System
ISO	Information System Owner
ISSO	Information System Security Officer
IT	Information Technology
NAMS	NASA Access Management System
NASA	National Aeronautics and Space Administration
NIST	National Institute of Standards and Technology
NPD	NASA Policy Directive
NPR	NASA Procedural Requirement
ODIN	Outsourcing Desktop Initiative for NASA
SATERN	System for Administration, Training, and Educational Resources for NASA
SDLC	System Development Life Cycle
SOC	Security Operations Center
SP	Special Publication