

NASA Information Technology Requirement

NITR 2810-14A

Effective Date: August 17, 2009

Expiration Date: May 16, 2011

Managing Elevated User Privileges on NASA IT Devices

Responsible Office: OCIO/Office of the Chief Information Officer

Table of Contents

Change History

PREFACE

- P.1 PURPOSE
- P.2 APPLICABILITY
- P.3 AUTHORITY
- P.4 APPLICABLE DOCUMENTS
- P.5 CANCELLATION

REQUIREMENT

RESPONSIBILITIES

Distribution

NODIS

Change History

NITR 2810-14A, Managing Elevated User Privileges on NASA Computers

Change Number	Date	Change Description
NITR 2810-14A	8/17/09	Removed compliance due date and refined: <ul style="list-style-type: none"><li data-bbox="604 558 1373 625">• Requirements for requesting elevated privileges (including training, and naming convention for custom workflows) and<li data-bbox="604 634 964 667">• Roles and responsibilities.

PREFACE

P.1 PURPOSE

a. The purpose of this policy is to ensure that every user of NASA information systems has the minimum level of administrative rights or privileges needed to successfully perform their authorized tasks, and to ensure that NASA has a record of who has elevated privileges on its information systems and for what reason. In adherence with federal regulations, NASA requirements, and security best practices, these measures are intended to reduce the risks to NASA's information and information technology (IT) resources, to ensure user accountability, and to appropriately manage NASA's IT environment.

b. Accessing information systems with elevated user privileges greatly increases the risks of security incidents and of unintended and/or detrimental changes to system configurations. For example, most viruses, trojans, and spyware install and run under the rights and privileges of the currently logged on user. When a user logs on to his/her desktop computer with elevated privileges, surfs the Web, and unknowingly downloads malicious software, this malware can install and run with elevated privileges, increasing the potential damage. In another example, a user accessing an IT device with elevated privileges has a much greater ability to inadvertently or maliciously change the configuration of the IT device, potentially creating security risks for the IT device and its environment, bringing the IT device out of compliance with NASA standard configurations, or rendering the IT device unusable.

P.2 APPLICABILITY

a. This NASA Information Technology Requirement (NITR) applies to all NASA facilities, employees, contractors (as provided by law or contract), recipients of NASA grants and cooperative agreements, partners and visitors, in achieving NASA missions, programs, projects, and institutional requirements.

b. The requirements of this document apply to:

- (1) Any access to a NASA IT device with elevated privileges, except where otherwise noted;
- (2) IT devices that have multiple privilege level capabilities; and
- (3) Elevated privileges at the operating system (OS) level. Elevated privileges at the application level are not within the scope of this document.

P.3 AUTHORITY

Reference paragraph P.3, NPR 2810.1A, Security of Information Technology.

P.4 APPLICABLE DOCUMENTS

a. NASA NPR 2810.1, Security of Information Technology.

b. NASA Memo "Meeting NASA Information Technology Security Requirements", July 2006.

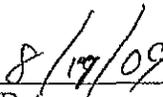
- c. NASA Security Handbook: ITS-HBK-0004 Implementation Guidance for NITR 2810-14A
- d. NITR 2800-1, NASA Information Technology Waiver Requirements and Procedures

P.5 CANCELLATION

- a. Cancels NITR 2810-14 "Managing Elevated User Privileges on NASA Desktop and Laptop Computers", September 2008.
- b. This NITR is cancelled by the next version of the NPR 2810.1.



Bobby German
Chief Information Officer (Acting)



Date

1.0 REQUIREMENTS

1.1 Anyone who accesses a NASA information system with elevated privileges shall be required to have authorization to hold these privileges.

1.2 Elevated privileges on a NASA information system shall only be granted to users who are qualified to access the information system with elevated privileges, commensurate with the level of elevated privileges being granted and the specific risks associated with the privileged access.

1.3 Qualification requirements for holding elevated privileges on a NASA information system shall be met as follows:

a. Users renew all applicable SATERN training once a year and/or maintain current all relevant industry certifications

b. All users granted elevated privileges demonstrate knowledge of the following topics, which can be achieved by obtaining and maintaining a SATERN training certificate in Elevated Privileges on NASA Information Systems:

(1) 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;

(2) Best practices and precautions to be used when accessing an IT device with elevated privileges;

(3) User responsibilities associated with accessing a NASA information system with elevated privileges; and

(4) Ramifications of user actions when accessing a NASA information system with elevated privileges.

1.3.1 In addition to the qualification requirements in section 1.3.a and 1.3.b, users granted elevated privileges for a period exceeding 30 days (for one authorization or, cumulatively, for multiple authorizations within a period of one year) shall demonstrate knowledge of the following topics. This can be achieved by obtaining and maintaining a SATERN training certificate in, "IT Security For Systems Administrators – Beginners Level," or by completing commensurate certifications and/or classroom or one-on-one training.

a. 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)

b. Security Program Management Compliance (including understanding the purpose of and elements of the IT Security Program; applying IT Security program elements to the information system; identifying areas of weakness in the IT Security Program)

c. 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 the 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 that it is being connected to; knowing the IT security responsibilities of users of the system; monitoring systems to identify potential IT security incidents; understanding and meeting all data retention and disposal requirements; etc.)

1.3.2 In addition to the qualification requirements in section 1.3.1, users granted elevated privileges in order to perform the duties of a system administrator shall demonstrate knowledge of the following topics. This can be achieved by obtaining and maintaining a SATERN training certificate in, "IT Security For Systems Administrators – Intermediate Level," and a SATERN training certificate in Operating System Security for the relevant operating system, or by completing commensurate certifications and/or classroom or one-on-one training.

- a. Incident Response (including making decisions on whether policy has been breached and if further action is needed)
- b. Security Program Management Compliance (including interpreting compliance with NASA's IT Security Program and analyzing patterns of non-compliance)
- c. Security components of each phase in the Systems Development Lifecycle (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; knowing how to conduct proper archiving, sanitizing, or disposition of all hardware, software, data, and facility resources; etc.)

1.4 Elevated privileges on a NASA information system shall only be used for the intended purposes for which they were granted.

1.5 All authorizations for elevated privileges shall be documented and managed in the NASA Account Management System (NAMS).

1.6 Each SSP shall reference the NAMS workflow being used to document and manage elevated user privileges for the information system.

1.7 The NASA SOC shall be notified of any NAMS workflows used to manage EP and the corresponding systems and/or applications so that the SOC can access all records of elevated privileges for incident management purposes.

1.8 All NAMS workflows used to document and manage elevated user privileges shall require, at minimum, the following information in the specified standard fields:

- a. Business Justification: This field shall be used to explain the user's business need for elevated privileges and to list the specific activities for which the user requires the requested privileges.
- b. Expiration date: The maximum expiration date of elevated user privileges is one (1) year from the time of the authorization but this time should be limited to as short a time period as possible.
- c. User Acknowledgement Statement acceptance: This field shall be used to indicate the user's acknowledgement of risks and user responsibilities associated with elevated privileges.

1.9 To obtain a waiver from any of the above requirements, the requester shall follow the waiver process as identified in NITR 2800-1.

a. Waivers of any requirements related to management of elevated user privilege shall be for specific IT devices, specific information systems, or specific individuals requesting elevated privileges

b. Waivers shall also be for specific time periods, not to exceed one year.

1.10 Additional implementation guidance is provided in NASA Security Handbook, ITS-HBK-0004, "Implementation Guidance for NITR 2810-14A."

2.0 RESPONSIBILITIES

2.1 The Center CIO shall:

- a. Review and approve/deny all requests for elevated user privileges.
- b. Have the 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.
- c. Verify that qualification requirements have been met before approving a request for elevated user privileges

2.1.1 The Center CIO may:

- a. Delegate responsibility for review and approval of requests for elevated user privileges, to the Center IT Security Manager (ITSM) or other NASA staff, but not to the account issuer.
- b. May revoke elevated privileges prior to the expiration date of the authorization.

2.2 The Information Technology Security Manager (ITSM) or designee may suspend elevated privileges prior to the expiration date of the authorization.

2.3 The Information System Owner (ISO) shall:

- a. Have the authority to deny elevated user privileges on his/her information system.

- b. Manage elevated user privileges on his/her NASA information systems in accordance with this policy and the established procedures.
- c. Ensure elevated user privileges are removed after the authorization has expired.
- d. Develop procedures for granting and removing elevated user privileges on the relevant system in accordance with this policy.
- e. Have the authority to approve elevated user privileges on their information system in an emergency situation.
- f. Limit the time period for emergency approvals to the time needed to deal with the particular emergency.

2.3.1 The ISO may:

- a. Delegate responsibility for review and denial of requests for elevated user privileges, to the Information System Security Officer (ISSO) or other staff, but not to the account issuer.
- b. Revoke elevated privileges prior to the expiration date of the authorization.

2.4 The Information System Security Official (ISSO) shall ensure:

- a. Periodic reviews are conducted to validate accounts only have the privileges for which a current authorization is available, and
- b. The use of elevated privileges is conducted in a form consistent with the usage justification.

2.4.1 The ISSO may revoke elevated privileges prior to the expiration date of the authorization.

2.5 The User shall:

- a. Obtain and maintain the necessary qualifications as required under this policy.
- b. Use elevated user privileges, once granted, only for the purposes intended, documented and approved in the request.
- c. 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.

APPENDIX A. Definitions

Term	Definition
Account Issuer	The entity that provisions/implements the elevated privilege request
Application Administrator	A person who manages a multi-user computer application or server software, for example, a database server or a web server. The application administrator performs administrative and maintenance related to the application. Some administrative and maintenance tasks may need the application administrator to have elevated privileges at the OS level.
Elevated privileges	<p>Elevated privileges are any access rights or permissions that allow the user that holds them to access system control, monitoring, or administration functions. This includes functions such as installing, upgrading, significantly changing or patching software, including the computer's operating system. For example, on Windows computers, elevated privileges include any rights or permissions other than those granted by membership in the Windows local "Users" group.</p> <p>See also: <i>Privileged Access, Privileged Account, Privileged Command, and Privileged User.</i></p>
Information System	<p>A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.[44 U.S.C., Sec. 3502]</p> <p>(Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.) [NIST]</p>
Information System Owner	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system. [NIST]
Information System Security Official	Individual assigned responsibility for maintaining the appropriate operational security posture for an information system or program. [CNSSI 4009]
Information Technology Security Manager	NASA Center Senior Information Security Officer responsible for assisting the Center CIO in implementing this directive, NASA information security policies and procedures, and the Federal information security laws, directives, policies, standards, and guidelines and compliance with the FISMA section 3541 et seq..
IT Device	A network endpoint or node regardless of its operating system or type, such as a desktop, laptop, server, printer, including network

	infrastructure hardware (firewall, router, switch, hub, etc.).
Multi-user system	A computer with an operating system that supports multiple users at once and/or different times. Examples include Windows workstations and servers, Unix/Linux systems)
Privileged Access	That which is granted to a user so that files, processes, and system commands are readable, writable, executable, and/or transferable. This allows a user to bypass security controls.
Privileged Account	An information system account with authorizations of a privileged user. [NIST]
Privileged Command	A human-initiated command executed on an information system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information. [NIST]
Privileged Function	A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. [CNSSI 4009]
Privileged User	Individual who is authorized to enter one or more privileged commands. Individual who has access to system control, monitoring, or administration functions often based on an assigned role (e.g., system administrator, information system security officer, maintainer, system programmer). [CNSS Inst. 4009, Adapted]
System administrator	A person who manages a multi-user computer system. Responsibilities are similar to that of a network administrator. A system administrator would perform systems programmer activities with regard to the operating system and other network control programs. [NPR 2810.1B]
System Security Plan	Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements. [NIST SP 800-18]
User	Individual, or (system) process acting on behalf of an individual, authorized to access an information system. [CNSS Inst. 4009, adapted]

APPENDIX B. Acronyms

CIO	Chief Information Officer
ISO	Information System Owner
ISSO	Information System Security Official
ITS-HBK	Information Technology Security Handbook
ITSM	Information Technology Security Manager
NAMS	NASA Account Management System
SATERN	System for Administration, Training and Educational Resources at NASA
SDLC	System Development Lifecycle
SSP	System Security Plan