

NASA Information Technology Requirement

NITR 2810-14

Effective Date: September 11, 2008

Expiration Date: September 11, 2011

**Managing Elevated User Privileges on NASA Desktop and Laptop
Computers**

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 2810-14, Managing Elevated User Privileges on NASA Desktop and Laptop Computers

Change Number	Date	Change Description
1	3/19/08	Initial
2	4/7/08	Formatting changes and revisions based on initial comments
3	7/7/08	Changes based on ITMB decisions
4	9/10/08	Edits to clarify approvals, training requirements

PREFACE

P.1 PURPOSE

NASA protects its Information Technology (IT) resources by employing skilled staff who are responsible and accountable for the installation, operation, and maintenance of desktop and laptop computers. NASA also applies sound security principles to the configuration and operation of these computers. The purpose of this policy is to limit user access with elevated privileges to desktop and laptop computers as much as possible to minimize IT security exposure.

P.2 APPLICABILITY

This document 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.

The requirements of this document apply to any access to NASA desktop or laptop computer systems. Elevated privileges on NASA servers are covered under those computers' System Security Plans, rather than this document.

NASA desktop or laptop computers are defined as all such computers that are used to store and/or process NASA information and are covered under a NASA IT Security Plan.

P.3 AUTHORITY

The NASA Chief Information Officer (CIO) has the authority to develop, implement, and manage IT processes and procedures to protect the confidentiality, integrity, and availability of NASA's IT resources. The CIO shall ensure that NASA's IT policy and requirements are developed in a way that is consistent with the applicable statutory authority, including the Federal Enterprise Architecture, the Clinger-Cohen Act and the Federal Information Security Management Act (FISMA); with regulatory requirements and external guidance, including Office of Management and Budget policy and Federal Information Processing Standards (FIPS) publications promulgated by the National Institute of Standards and Technology (NIST); and with internal NASA policies and requirements.

P.4 APPLICABLE DOCUMENTS

- a. NASA NPR 2810.1, Security of Information Technology
- b. NASA Memo "Meeting NASA Information Technology Security Requirements", July 2006

P.5 CANCELLATION

None


Jonathan Q. Pettus
Chief Information Officer

9-10-08
Date

REQUIREMENT

Elevated user privileges shall be managed on all NASA desktop and laptop computers. User access with elevated privileges includes any access to the computer that allows the user to install, upgrade, significantly change or patch software, including the computer's operating system.

Elevated user privileges shall only be approved and granted for users with a documented requirement, for a specified time period not to exceed twelve months.

The NASA Account Management System (NAMS) shall be used to submit and approve/deny all requests for elevated user privileges.

All NASA desktop and laptop computers shall be in compliance with this policy no later than 1 June, 2009.

To obtain elevated users privileges on a NASA desktop or laptop:

- The user shall obtain and maintain a current SATERN training certificate in Basic IT Security for System Administrators, or equivalent classroom or one-on-one training
- If the time period specified in the request, or the combined time specified in multiple requests by the same user, exceeds one month, the user shall also obtain and maintain
 - a current SATERN training certificate in Intermediate IT Security for System Administrators or equivalent classroom or one-on-one training, and
 - a current SATERN training certificate in Operating System Security for the relevant operating system or equivalent classroom or one-on-one training.
- The relevant Center Chief Information Officer (CIO), or designee, shall review and approve/deny the request for elevated user privileges.
- Upon approval of the request for elevated user privileges, the required privileges shall be granted.
- Upon completion of the required tasks or at the end of the specified time period, the elevated user privileges on the computer shall be revoked unless training and authorization are renewed.

RESPONSIBILITIES

The Center CIO

- Shall verify that training requirements have been met before approving a request for elevated user privileges
- Shall review and approve/deny all requests for elevated user privileges
- May delegate responsibility for review and approval of requests for elevated user privileges, but not to the information system owner (ISO) or staff of the relevant system
- May grant a waiver, or an extension to the specified time period, of no more than 90 days.

The user

- Shall complete and maintain the necessary training requirements
- Shall complete a request for elevated users privileges, including documentation and justification of the access requirement, and submit the request to the Center CIO
- Shall use elevated user privileges, once granted, only for the purposes documented and approved in the request
- Shall be responsible for service reinstatement fees incurred for remediation necessary as a result of inappropriate actions performed on the desktop or laptop during the user's access with elevated privileges.

The ISO

- Shall develop procedures for granting and removing elevated user privileges on the relevant system in accordance with this policy
- Shall manage elevated user privileges on all NASA desktop and laptop computers under his/her purview in accordance with this policy and the established procedures
- Shall ensure elevated user privileges are removed after the specified time period has elapsed.