Nuclear Regulatory Commission
Office of the Chief Information Officer
Computer Security Standard

Office Instruction:	**CSO-STD-2006**
Office Instruction Title:	**User Access Management Standard**
Revision Number:	**2.0**
Effective Date:	**January 31, 2019**
Primary Contacts:	**Jonathan Feibus**
Responsible Organization:	**OCIO/CSO**
Summary of Changes:	CSO-STD-2006, “User Access Management Standard,” provides the minimum requirements that must be met for user access to NRC computer system resources./
Training:	As requested

Approvals			
Primary Office Owner	Office of the Chief Information Officer (OCIO) / Computer Security Organization (CSO)	**Signature**	**Date**
SWG Chair	Bill Bauer	/RA/	12/7/18
CISO	Jonathan Feibus	/RA	12/10/18

TABLE OF CONTENTS

Computer Security Standard
CSO-STD-2006

User Access Management Standard

---

1 PURPOSE

CSO-STD-2006, “User Access Management Standard,” provides the minimum security requirements that must be applied to all users accessing any system operated by or on behalf of the Nuclear Regulatory Commission (NRC) processing information, up to and including, the classified level, to ensure the security of NRC information and system resources.

This standard is intended to be used by system administrators and Information System Security Officers (ISSOs) to ensure that user access is managed.

2 GENERAL REQUIREMENTS

This standard applies to user access to NRC information and system resources, whether the resource is operated by or on behalf of NRC. User accounts are characterized as either privileged or non-privileged. A privileged user is authorized (and therefore, trusted) to perform security relevant functions that general users are not authorized to perform. Whereas, a non-privileged user is authorized general user access to system resources that is controlled in a way that does not permit those controls and rules to be changed or bypassed by a general user.

All aspects of user access must be managed, from requesting initial access to the final stage of de-registering users who no longer have a need for access.

In addition, policies, processes, and procedures must also address requirements for privileged or non-privileged user access, as specified in CSO-STD-0020, “Organization-Defined Values for System Security and Privacy Controls.”

3 SPECIFIC REQUIREMENTS

Privileged users exercise primary responsibility for user access management and are individuals entrusted with the ability to set and bypass system security controls. Examples of privileged users include those assigned one or more of the following functions:

- ISSO
- System administrator (e.g., workstations, servers, domain controllers)
- Network administrator
- Database administrator

3.1 Management of User Access

System owners must ensure the following requirements are met:

- All users are uniquely identified and authenticated to systems and networks before gaining system access, except as noted below for shared user identifications (IDs). Access controls must then be used to grant access based on the user ID and the access permissions associated with that ID.
- Type of user accounts permitted for system access are defined. The account types are: non-privileged user, privileged user, shared/group account, system, service, emergency, or temporary accounts. These account types are defined in CSO-STD-0020.
- User system roles are both clearly defined and the type of system access (e.g., create, modify, delete, authorize transaction) identified for each role.
- Users have undergone appropriate background checks, clearance processing, and security training required for the highest level of information processed by the system prior to granting system access, in accordance with Management Directive (MD) 12.3, "NRC Personnel Security Program," and MD 12.5, "NRC Cybersecurity Program."
- Development of system access agreements in accordance with CSO-STD-0020, PS-6, "Access Agreements."
- Number of user accounts that provide the ability to set and bypass system security controls is kept to a minimum consistent with operational requirements.
- Privileged access users with accounts (e.g., ActiveRoles Server "AR" accounts) residing within the NRC enterprise directory server consent to the applicable Rules of Behavior (RoB).

Also, system owners may grant use of a shared user ID for general user access when the system does not contain or access any sensitive information or systems (e.g., a standalone training laptop).

3.1.1 User Registration and Account Management

User registration involves all steps necessary to provide users with appropriate access to systems. The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63-3, "Digital Identity Guidelines," will also apply with respect to user registration of non-NRC contractor/employee users (e.g., users from licensees, agreement states, members of the public). Account management involves the steps required to ensure user access and authorizations are continuously appropriate, including removing access that is no longer appropriate.

System owners must ensure the following requirements are met:

- Formal user registration and account monitoring procedure is established and documented for the system. The procedure must include the following:
  - User roles applicable to the system (e.g., data entry personnel, data approvers);
  - Criteria to determine if a user meets the qualifications for each user role. Qualifications include, but are not limited to:

        - Required background checks/clearances,
        - Knowledge,
        - Skills, and
        - Abilities to perform the tasks associated with the user role;
    - Criteria to ensure privileges are assigned to user roles in a manner that assures required separation of duties;
    - Privileges and accesses associated with each user role;
    - Circumstances for modification or removal of access (i.e., change in job responsibilities, disciplinary action, transfer, or termination of employment); and
    - Circumstances for modification or removal of privileges associated with a change in user role or disciplinary action.
- Default user IDs are renamed where possible.
- User IDs have associated authentication information that is different from the default provided by the vendor.
- System-defined guest, anonymous, and other optional generic accounts (that allow non-unique user IDs) are prohibited and are disabled, except as specifically approved by the Authorizing Official (AO).

3.1.2 Management of Privileges

System owners must ensure the following requirements are met:

- Privileged users have separate accounts as follows:
    - A privileged account, or accounts (where privileged accounts are separated based upon their roles), that is only used for specific job-related activities that require privileges; and
    - A non-privileged (general user) account to perform general user activities.
- Number of individuals assigned to distinct types of privileged accounts is kept to a minimum consistent with operational requirements.
- Non-privileged accounts are prevented from modifying system-level files and accessing system information and resources.
- Access to system information defining network options, resources, and operator profiles is restricted to system auditors, system administrators, and ISSOs.
- Access and access privileges to sensitive information is limited to those that need the information to perform their job-related duties.
- Each user is only granted those accesses necessary for the user to perform his/her duties on each computer system. The concept of least privilege is universally accepted as a basis for security. The application of this principle limits the damage that can result from accident, error, or unauthorized use.
- Personnel performing auditor functions are only afforded read access. Auditors may not modify or write to any information technology (IT) systems being audited.

Application/service accounts must only be granted the minimum privileges required in accordance with the principal of least privilege.

Also, where possible, a Just in Time (JIT) privilege management (e.g., in Windows environment) should be used to grant privileged users access to carry out functions (e.g., install/upgrade software or patches). JIT administration allocates user privileges to resources for a limited period only. Thereby, in case of a breach, this restriction could limit or eliminate the chance of compromise to additional devices/systems. If JIT administration is not used, privileged access should be segmented based upon roles (e.g., separate privileged accounts for workstations, member server, domain controller, and network administration).

3.2 Review of User Accounts and Access Rights

System owners must ensure the following requirements are met:

- A list of authorized users is maintained for each system, including updates or removal upon change in user reassignment or termination.
- NRC staff and contractor access are disabled in accordance with CSO-STD-0020, PS-4," Personnel Termination," for any voluntary or involuntary termination.
- Access to the system is updated in accordance with CSO-STD-0020, PS-5, "Personnel Transfer," for any reassignment of NRC staff or contractors.
- Periodic user account reviews are conducted in accordance with CSO-STD-0020, AC-2, "Account Management."

APPENDIX A. ACRONYMS

AO	Authorizing Official
AR	ActiveRoles
ID	Identification
IT	Information Technology
ISSO	Information System Security Officer
JIT	Just in Time
MD	Management Directive
NIST	National Institute of Standards and Technology
NRC	Nuclear Regulatory Commission
RoB	Rules of Behavior
SP	Special Publication

APPENDIX B. GLOSSARY

Non-privileged User Account	User has controlled access to the system resources in such a way that he/she cannot change or by-pass these controls.
Privilege Management	The practice of controlling and administering digital user identities and the rights of those identities to perform actions on specified resources.
Privileged User Account	User has access to system control, monitoring, or administration functions (e.g., system administrator, system ISSO, system programmers).
User	An authorized individual that logically accesses an IT system in an approved fashion.
User Access	Making use of a system after successful identification and authentication to the system.
User System Role	The type of function a system user performs (e.g., data input, authorize financial expenditures, system administrator).
User ID	The identifier the system associates with a specific user.

CSO-STD-2006 Change History

Date	Version	Description of Changes	Method Used to Announce & Distribute	Training
20-Jan-10	1.0	Initial issuance	Distribution at ISSO forum and posting on CSO web page	Upon request
21-Apr-11	1.1	Augmented to incorporate logical access controls and removed items defined within the organizational defined values standards		
10-Dec-18	2.0	Updated with latest requirements.	Post to OCIO/CSO web page.	Upon request