The National Science Foundation
Polar Programs
United States Antarctic Program

Information Resource Management Directive 5000.07
User Access Control Policy

Organizational Function	Information Resource Management	**Policy Number**	5000.07
		Issue Date	1 August 2004
Policy Category	Information Security Policies and Instructions	**Effective Date**	1 August 2004
		Updated	15 May 2012
Subject	User Access Control	**Authorized By**	Section Head, NSF/GEO/PLR/AIL
Office of Primary Responsibility	National Science Foundation Geosciences Directorate Division of Polar Programs Antarctic Infrastructure & Logistics	**Responsible Officials**	Primary Responsibility: Mr. Patrick D. Smith Technology Development Manager Security Responsibility: Ms. Desari Mattox USAP Information Security Manager
Address	Suite 755 4201 Wilson Blvd Arlington, VA 22230	**Phone** **Fax** **Web**	703.292.8032 703.292.9080 http://www.nsf.gov/div/index.jsp?div=PLR
Distribution	USAP-Wide	**Status**	Final Policy
Online Publication	http://www.usap.gov/technology/contentHandler.cfm?id=1563		

1. PURPOSE

This directive establishes the policy for managing user access to information systems supporting the National Science Foundation (NSF), Geosciences Directorate (GEO), Polar Programs (PLR), United States Antarctic Program (USAP). The purpose is to ensure the necessary user access controls are in place for controlling the actions, functions, applications, and operations of legitimate users. The aim is to protect the confidentiality, integrity, and availability of all USAP information resources.

2. BACKGROUND

Federal regulations require USAP information resource managers to establish user access controls to protect information resources. Such controls will be based on the principle of least privilege, defined as granting the most restrictive authority so that users are not allowed to undertake actions beyond what their duties require. User access issues also involve Information Categorization issues addressed in USAP Information Security Policy 5000.3, *USAP Information Categorization.*

3. GUIDING PRINCIPLES

- Users will have access to the resources needed to accomplish their duties.
- User access applies the principles of least privilege and resource categorization as necessary tools to achieve the desired purpose
- User access controls will balance security and mission needs.

4. POLICY

All managers of USAP information resources will ensure access to USAP information is properly authorized and granted with correct access levels and privileges applied.

4.1 Operational Definitions

4.1.1 Authentication: Verification that the user's claimed identity is valid and is usually implemented through a user password at logon.

4.1.2 Discretionary User Access: The ability to manipulate data using custom or general-purpose programs. The only information logged for discretionary control mechanisms is the type of data accessed and at what level of authority.

4.1.3 Identification: The act of a user professing an identity to a system, usually in the form of a logon to the system.

4.1.4 Non-discretionary User Access: The access obtained in the process of specific business transactions that affect information in a predefined way. For example, USAP deployment specialists need to access participant information to make travel arrangements, but may not need the ability to change any existing information.

4.1.5 Password: An arrangement of characters entered by a system user to substantiate their identity, authority, and access rights to an information system they wish to use.

4.1.6 Privilege: The level of user authority or permission to access information resources. Privileges can be established at the folder, file, or application levels, or for other conditions as applicable.

4.1.7 Special User Access Privileges: Privileges that allow users to perform specialized tasks that require broad capabilities. For example changing control functions such as: access control, logging, and violation detection, require special access privileges.

4.1.8 User Account: An issued name with authority, granted to an individual to access a system or software application. System administrators, with proper management approval, typically grant user accounts. To access an account, a user needs to be authenticated, usually by providing a password.

4.1.9 User Access Controls: The rules and deployment of mechanisms, which control access to information resources, and physical access to premises.

4.2 User Accounts

The creation of a user account must be initiated through a request from personnel authorized to approve access to the specified resources, typically a manager or supervisor.

4.3 Account Management

Each USAP participant organization manages user accounts for USAP systems within their area of responsibility. Records of processed and denied requests for creation of user accounts must be kept for auditing purposes. Records will be retained for one year, unless otherwise specified by NSF.

4.4 User Accounts Characteristics

All USAP user accounts must be unique, and traceable to the assigned user. All USAP participant organizations will take appropriate measures to protect the privacy of user information associated with user accounts. The use of group accounts and group passwords is not allowed, unless specifically approved by NSF PLR.

4.5 Password Reset

Each USAP participant organization will establish a procedure for verifying a user's identity prior to resetting their password.

4.6 User Account Privileges

Users will be granted the minimum access required to perform their specific tasks. Granting access levels to resources shall be based on the principle of least privilege, job responsibilities, and separation of duties. The level of minimum access requires the recommendation of the user's manager, and the evaluation of the information system owner. The information system owner will have final determination as to the level of a user's access for their system.

4.7 Inactive Accounts

Accounts will be disabled after 30 days of inactivity. Users planning to deploy to field operating locations or to be away from the office for other approved periods of extended absence should coordinate their absence with the account manager to ensure proper disposition of the account.

4.8 Temporary User Accounts

All requests for temporary user accounts shall provide an expiration date to be applied at the time the account is created.

4.9 Password Characteristics

All passwords must be constructed using the following characteristics: alphanumeric characters, with a mixture of letters, numbers and special characters. Each USAP participant organization will implement appropriate procedures and technology to enforce this requirement.

4.10 Automatic Logon

The use of automatic logon software to circumvent password entry shall not be allowed, except with specific approval from the Information Security Manager, for special tasks such as automated backups.

4.11 User Account and Password Safekeeping

Each individual assigned a user account and password is responsible for the actions taken under said account, and must not divulge that account information to any other person for any reason

4.12 Management Access to User Accounts

Management access to user accounts will be limited to business purposes only, such as during an emergency or contingency situation, cases of extended user absence, or user abuse of USAP information resources. Each participant organization will establish procedures for providing their management with access to accounts assigned to a user within their organization. These procedures will be coordinated with the NSF OPP and USAP Information Security Manager.

4.13 Transfers

Personnel transferring from one area of responsibility to another, shall have their access accounts modified to reflect their new job responsibilities.

4.14 User Access Cancellation

Each USAP participant organization will implement procedures to immediately cancel account access and physical access for users whose relationship with the USAP has concluded, either on friendly or unfriendly terms.

4.15 User Session Time-out

User sessions will time-out after 15 minutes of inactivity unless otherwise specified as part of the system or application security plan. This includes user connections to the Internet, or to specific applications.

4.16 Remote Access Security

Access points for remote computing devices shall be configured using necessary identification and authentication technologies to meet security levels of physically connected computers.

4.17 New Information Systems

All new information systems acquired or developed by USAP organizations to support program requirements will incorporate access controls to properly protect the USAP information resources.

4.18 Sensitive Information Access

Individuals for positions with access to sensitive information will be screened for best suitability to the position. These individuals will be subject to the provisions of USAP policies and procedures to protect and safeguard such information from unauthorized disclosure.

4.19 Temporary Access to Sensitive Resources

Temporary access to resources categorized as sensitive will be set with expiration dates where possible. The system owner will monitor temporary access to ensure activities comply with the intended purpose.

5. APPLICABILITY AND COMPLIANCE

This policy applies to all information resources, systems, and technology and to all users of these resources, systems and technology within the USAP operating environment or connected to the USAP information infrastructure. Compliance with this policy is as indicated in USAP Information Resource Management Directive 5000.01, The USAP Information Security Program.

6. RESPONSIBILITIES

6.1 USAP Information Security Manager (ISM)

The ISM coordinates the activities of USAP participant organizations in the implementation of this policy.

6.2 USAP Participant Organizations

Each USAP participant organization will establish procedures to implement these requirements.

7. PROGRAM IMPLEMENTATION

Each participant organization will establish processes and procedures to implement this policy, and coordinate their activities with the USAP Information Security Manager.

7.1 User Access Administration

The information system owner has primary management responsibility for administering user access to USAP information resources. The information system owners in each USAP participant organization will coordinate their activities with the USAP Information Security Manager.

8. AUTHORITY

This directive is published in conformance with the authority of the National Science Foundation Act of 1950, as amended and extended, the Federal Information Security Management Act of 2002, and NSF guidance.

Brian Stone
Section Head, NSF/GEO/PLR/AIL

bstone@nsf.gov

Digitally signed by bstone@nsf.gov
DN: cn=bstone@nsf.gov
Date: 2014.05.22 19:47:38 -04'00'

REVISION/CHANGE RECORD

Pages	Date	Version	Author/Reviewer	Reason for Change
All	6/9/2011	1.0	Matthew Rogers	Verified alignment with NIST Special Publication 800-53 Revision 2. Changed ISM name.
All	5/3/2012	2.0	Alex Jerasa	Updated key contacts and conducted FY12 review
All	5/15/2013	3.0	Desari Mattox	Updated OPP and AIL titles to align with NSF re-organization & Verify alignment with NIST SP 800-53 rev 3.