



The National Science Foundation
Office of Polar Programs
United States Antarctic Program

Information Resource Management Directive 5000.10
USAP Personnel Security Policy

Organizational Function	Information Resource Management	Policy Number	5000.10
		Issue Date	1 August 2004
Policy Category	Information Security Policies and Procedures	Effective Date	1 August 2004
		Updated	24 April 2007
Subject	Personnel Security Policy	Authorized By	Director, OPP
Office of Primary Responsibility	National Science Foundation Office of Polar Programs Antarctic Infrastructure & Logistics	Responsible Official	Mr. Patrick D. Smith Technology Development Manager
Address	Suite 755 4201 Wilson Blvd Arlington, VA 22230	Phone	703.292.8032
		Fax	703.292.9080
		Web	www.nsf.gov
Distribution	USAP-Wide	Status	Final Policy
Online Publication	www.usap.gov		

1. PURPOSE

This directive establishes the policy for Personnel Security as it relates to information systems supporting the National Science Foundation (NSF) Office of Polar Programs (OPP), United States Antarctic Program (USAP).

2. BACKGROUND

Federal information technology regulations require USAP information systems to develop and implement a Personnel Security Plan to ensure each individual is granted access to information resources commensurate with their job responsibilities. Adherence to this policy improves information confidentiality and integrity and protects government and private resources used to execute and administer mission activities while allowing effective access to program information by the general public.

3. GUIDING PRINCIPLES

- Personnel security measures will be designed to protect the confidentiality, integrity, and availability of USAP information resources.
- Personnel assigned to sensitive or critical positions will be held to a higher expectation of trust, commensurate with their responsibilities, than those assigned to a position not considered sensitive or critical in nature.

4. POLICY

This policy establishes the requirements for a program that determines the sensitivity of positions, and screens individuals who participate in the design, operation, or maintenance of information systems.

4.1 Operational Definitions

4.1.1 Confidentiality

Confidentiality of information relates to the authorized access to or disclosure of information. Confidentiality is maintained by not making it available or disclosing it to unauthorized individuals, entities, or processes.

4.1.2 Critical Position

A critical position is responsible for accomplishing a critical task or activity in support of an information resource, which, if left unaccomplished or compromised, could result in injury or loss of life, significant impact to the USAP mission, significant loss of government resources, or unauthorized access to or disclosure of Privacy Act, proprietary, or other sensitive information.

4.1.3 Least Privilege

An information security principle stating that users of information resources should only be granted the accesses they need to perform their job duties.

4.1.4 Personnel Controls

Personnel controls are the steps followed in the process of managing individuals identified for or assigned to a sensitive or critical position. Such controls may include background checks, job rotation frequency and sequence, and sanctions for unauthorized actions.

4.1.5 Personnel Screening

Personnel screening is the process of investigating the background of candidates to determine their suitability for a given job position.

4.1.6 Sensitive Information

Sensitive Information is any information, the loss, misuse, unauthorized disclosure, unauthorized access, or unauthorized modification of which, could adversely affect the

interest or the conduct of the USAP, or the privacy to which individuals are entitled under section 552a of Title 5, United States Code (the Privacy Act) (NIST SP 800-12, The NIST Handbook).

4.1.7 Sensitive Position

A sensitive position is a position responsible for accomplishing a task or activity which involves sensitive information. A sensitive position may not necessarily be involved in critical mission activities.

4.1.8 Separation of Duties

Separation of duties is the practice of dividing the steps in a critical function among different individuals. For example, one system programmer can create a critical piece of operating system code, while another authorizes its implementation. Such a control keeps a single individual from subverting a critical process.

4.2 Sensitive and Critical Activities, Roles and Positions

The OPP Technology Manager will work with the USAP ISM, the USAP Prime Contractor, and other USAP participant organizations to identify activities, roles, and positions within the USAP that are considered sensitive or critical in nature. The ISM will maintain a list of these activities, roles and positions for all USAP participant organizations. Activities, roles, and positions will be categorized as follows:

- **Category A: Basic information user:** A user of USAP information resources who does not normally work with sensitive information.
- **Category B: Sensitive information user:** A user of USAP information resources who normally works with sensitive information, such as human resource information, financial information, or medical information. Information technology system or network positions typically fall into this category.
- **Category C: Critical information responsibility:** A position of responsibility for information resources which, if the duties were not accomplished would result in injury or loss of life, significant impact to the USAP mission, or unauthorized access to or disclosure of sensitive information.
- **Category D: System owner or administrator:** A position of responsibility that involves the daily management of sensitive or critical information resources.

4.3 Least Privilege Concept

Managers in USAP participant organizations will apply the concept of Least Privilege to all sensitive and critical positions.

4.4 Personnel Screening & Evaluation

Individuals identified to fill a position, perform an activity, or act in a role that is considered sensitive or critical, such as system or LAN administrator, must satisfactorily complete a personnel screening process before being allowed to proceed with their sensitive or critical duties. The screening process is normally accomplished by the sponsoring organization, and may include a background investigation of varying levels of

detail as specified by OPP. Personnel whose job duties include access to sensitive information will be evaluated to assess their suitability for the position, and to ensure they understand the responsibility of protecting sensitive information and their expected behavior during the discharge of their duties.

4.5 Hiring, Firing, Release, and Transfer of Personnel

The ISM will coordinate the development of procedures by USAP participant organizations to address the hiring, firing, release, and transfer of personnel holding sensitive or critical positions. These procedures will address, among other things, issues related to non-disclosure agreements, and the management of sensitive information.

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 Security Policy 5000.1, *The USAP Information Security Program*.

6. RESPONSIBILITIES

In addition to the responsibilities identified in USAP Information Resource Management Directive 5000.1, The USAP Information Security Program, the following officials have specific responsibilities related to Personnel Security.

6.1 USAP Information Security Manager (ISM)

The ISM coordinates the development and implementation of a Personnel Security program that meets federal requirements.

6.2 USAP Information Systems Managers & Administrators

The managers and administrators of USAP information systems ensure all users of their systems have completed the appropriate Personnel Security processes and procedures.

7. PERSONNEL SECURITY PLAN IMPLEMENTATION.

7.1 Implementation

All USAP participant organizations will establish and maintain procedures to implement this policy.

7.2 Support from USAP Participant Organizations

The ISM will develop the necessary procedures for screening new personnel, and identifying the proper security controls for all positions. USAP Participant Organizations will support the ISM through the participation of their information technology, human resources, physical security, and other sections.

7.3 Policy Review

The USAP Information Security Manager will review this policy in conjunction with major changes to the information infrastructure, as part of the USAP's participation in agency security audits, after each breach in system security, or every two years. The ISM will submit policy changes and new policies for review and approval by NSF OPP.

8. AUTHORITY

Publication of this policy is 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 Manual 7, The NSF Information Security Handbook.

KARL A. ERB
Director