The National Science Foundation
Polar Programs
United States Antarctic Program

Acknowledgement of United States Antarctic Program Rules of Behavior for Sensitive Information and Personally Identifiable Information ICT_FRM-5000.24b

1 GENERAL INFORMATION

The purpose of the United States Antarctic Program (USAP) Rules of Behavior for Sensitive Information (SI) and Personally Identifiable Information (PII) is to highlight federal laws and guidelines from NSF and other federal documents for USAP participants with access to SI or PII.

Sensitive Information is information that has been characterized in accord with Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems* & National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60 Volume 1 rev 1, *Guide to Mapping Information and Information Systems to Security Catagories* as requiring access restrictions and protection from unauthorized disclosure. Basic types include:

- Privacy Act Systems of Records
- Personal medical information (PHI – Protected health information)
- Personal Identifiable Information
- Financial information
- Trade Secrets Act protected data
- Comercial proprietary data
- Operational Security (OPSEC) information
    - Current US Air Force and Air National Guard flight operation details
- IT infrastructure information
    - detailed internal USAP network diagrams
- Information Technology information
    - root or system administrator passwords to systems on the USAP network
    - vulnerability scan results
    - system log files

Personally Identifiable Information. *OMB M-07-16 defines "personally identifiable information" as information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of*

_____/_____
Initials Date

birth, mother's maiden name, etc. PII examples provided by NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* include but are not limited to:

- Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card number
- Address information, such as street address or email address
- Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry)
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

Federal laws and guidelines pertaining to SI and PII include:

- Privacy Act of 1974 (5 U.S.C. § 552a)
- E-Government Act of 2002 (44 U.S.C. 3601 *et seq.*)
- OMB Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*
- OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
- OMB Memorandum M-06-16, *Protection of Agency Sensitive Information*
- Federal Information Security Management Act (FISMA) of 2002 (44 U.S.C. § 3546)

The USAP Rules of Behavior for Sensitive Information and Personally Identifiable Information (SenROB) must be reviewed and signed by USAP participants with access to SI or PII. Signatories accept that they understand and take personal responsibility for the security of sensitive information and personally identifiable information.

The USAP SenROB is founded on the principles described in federal law, and other regulatory documents such as the Code of Ethics for Government Employees, Office of Personnel Management regulations, and Office of Management and Budget. Therefore the SenROB carries the same responsibility for compliance as the official documents cited above.

2 USER RESPONSIBILITIES

In the course of performing official duties, USAP participants with access to SI or PII are responsible for avoiding inappropriate access or disclosure of SI and PII of any kind and are bound to follow certain methods of storage and transmission for these kinds of data. These rules of behavior detail the responsibilities of and expectations for all individuals with access to SI or PII.

_____/_____
Initials Date

3 RESPONSIBILITY/ACCOUNTABILITY REQUIREMENTS

- Users should only use systems, software, and data for which they have authorization and use them only for official Polar Programs' business.
- Users with access to systems and data that utilize SI or PII must view and access this information only for the purposes for which use of the data is intended.
- Users must protect sensitive information from unauthorized disclosure.
- Users shall not store SI or PII on portable devices such as laptops, tablets, smart phones and USB drives or on remote/home systems unless approved encryption methods are employed.
- Users are prohibited from transmiting SI or PII via plain text e-mail; only approved encryption methods shall be used.
- All records containing SI or PII must be stored on network drives with access limited to those individuals or entities that require access to perform a legitimate job function.
- All removable or transportable media (e.g., paper forms, reports, cassettes, CDs, USB drives, etc.) containing SI or PII must be secured when not in use. Acceptable security measures depend on the circumstances, but may include locked file rooms, desks, cabinets and encryption.
- Subject to applicable document retention policies or unless required by law, when no longer required, paper documents and electronic media containing SI or PII must be destroyed or disposed of using methods designed to prevent subsequent use or recovery of information in accordance with NIST SP 800-88 Rev 1, *Guidelines for Media Sanitization* and USAP Directive 5000.22, *Media Protection Policy*.Organizations must follow their media sanitization procedures.
- In accordance with OMB Memorandum M-07-16, users must immediately report actual and potential incidents of inappropriate disclosure of SI or PII to the USAP Help Desk Toll Free at 1-800-688-8606 (Extension 32001) or (720)-568-2001 within 24 hours of detection.

USAP participants who have access to SI or PII must adhere to these rules and guidelines. I acknowledge receipt of, understand my responsibilities for, and will comply with the USAP Rules of Behavior for Sensitive Information and Personally Identifiable Information.

Signature of User	Date
Printed Name of User	Affiliation