**NATIONAL SCIENCE FOUNDATION**
4201 WILSON BOULEVARD
ARLINGTON, VIRGINIA 22230

**Acknowledgement of United States Antarctic Program Rules of Behavior for Sensitive Information and Personally Identifiable Information**

## SENSITIVE RULES OF BEHAVIOR

## 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.

SI is information sensitive to the security of the USAP program, including but not limited to:

- Information Technology information
  - detailed internal USAP network diagrams
  - root or system administrator passwords to systems on the USAP network
  - vulnerability scan results
  - system log files
- Detailed financial information
- Medical information when combined with PII information
- Operational security (OPSEC) information.
  - Current US Air Force and Air National Guard flight operation details

PII is information about an individual maintained by the USAP, including name and Social Security Numbers (SSN) and any other personal information which can be used to distinguish or trace an individual's identity.

Federal laws and guidelines pertaining to SI and PII include:

- Public law 93-579 – *Privacy Act*
- Public law 107-347 – *E-Government Act of 2002*
- OMB Memoranda M-03-22, M-06-16, and M-07-16

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 public 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.

## USER RESPONSIBILITIES

In the course of performing official duties, USAP participants with access to SI or PII specifically Social Security Numbers (SSN), are responsible for avoiding inappropriate access or disclosure of any kind and are bound to follow certain methods of storage and transmission for



_____/_____
Initials Date

these kinds of data. These rules of behavior detail the responsibilities of and expectations for all individuals with access to SI or PII.

## Responsibility/Accountability Requirements

- Users should only use systems, software, and data for which they have authorization and use them only for official USAP business.
- Users with access to systems and data that utilize SI or PII, specifically SSNs, must view and access this information only for the purposes for which use of the data is intended.
- Users must protect sensitive information from disclosure.
- Users shall not store SI or PII on portable devices such as laptops, PDAs and USB drives or on remote/home systems unless they have written authorization and encryption is employed.
- Users shall not transmit SSNs via e-mail unless encrypted and required by the USAP mission.
- Where possible, 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. Reasonable 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.
- 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

The USAP has taken steps to secure SI and PII within corporate databases. USAP participants who have access to retrieve SI or PII must adhere to these rules and guidelines. I acknowledge receipt of, understand my responsibilities, 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