

NATIONAL SCIENCE FOUNDATION
4201 WILSON BOULEVARD
ARLINGTON, VIRGINIA 22230

**Acknowledgement of Information Security Policies
&
Permission for Use of National Science Foundation/United States Antarctic Program
Information Systems and Services**

Scope of Authorization

Permission for use of National Science Foundation/United States Antarctic Program (NSF/USAP) information systems and services is restricted to authorized participants in the United States Antarctic Program, designated contractors and U.S. Government employees, official visitors, or individuals otherwise having an authorized purpose for gaining access to, and utilizing the services of, NSF/USAP owned, operated, or provided information systems and services. USAP information systems and services include, but are not limited to, those located at the support contractor's headquarters and at USAP facilities in Port Hueneme, CA; Christchurch, NZ; Punta Arenas, Chile; Antarctic stations and research vessels.

Agreement Provisions

Permission for use of NSF/USAP information systems and services requires the following acknowledgements:

1. Government owned system. The information systems of the United States Antarctic Program are National Science Foundation federal government owned information systems. When attaching or otherwise interconnecting personally or privately owned information systems with government systems, the NSF reserves the right to extend its information security policies, Rules of Behavior, procedures, and guidance to these systems in order to ensure the integrity of NSF/USAP systems.
2. Mandatory awareness training. Individuals using NSF/USAP information systems and services must receive information security awareness training no less than once annually. Awareness training is a prerequisite for gaining permission to use NSF/USAP information systems and services and may be provided by verbal briefings, written reference materials, and/or on-line training systems. Permission to use NSF/USAP information systems and services may be suspended, revoked or denied, as appropriate, for individuals who have not fulfilled the mandatory awareness training requirement.
3. Only authorized use is permitted. Individuals using NSF/USAP information systems and services without authority, or in excess of their assigned authority, are subject to revocation of access privileges, in part or in whole. Further, access for purposes beyond authorization or assigned authority may be a violation of federal law. Penalties for misuse may include, but are not limited to, appropriate administrative sanctions, civil liability or criminal prosecution.
4. No expectation of privacy. Individuals using NSF/USAP information systems and services should be aware that they have no expectation of privacy. Files maintained in NSF/USAP information systems, including electronic mail files, may be reviewed by NSF officials who have legitimate reasons to do so when authorized by the Director or Deputy Director, or by the Inspector General. Individuals should be aware that NSF reserves the right to conduct work-related investigations for the purpose of investigating work-related misconduct, such as violations of the acceptable use policy.
5. Common Authority and Consent to be Monitored. In the course of conducting routine and corrective systems maintenance and administration, NSF designated systems technical personnel have legitimate work-related needs for access to files, contents of files, configuration data, and system log information, as well as monitoring of user activities. This extends to any personally or privately owned information systems attached to, or otherwise interconnected with, NSF/USAP systems such that the electronic exchange of information between the two is possible. If such work-related activities reveal possible evidence of criminal wrongdoing, NSF authorizes system personnel to provide the information gained from such activity to NSF officials for administrative action, with referral of such matters to law enforcement officials when appropriate.

6. Prohibition on tampering. Unless explicitly authorized by NSF designated personnel, individuals using NSF/USAP information systems and services do not have permission to physically access, modify, or alter configuration settings or in any way change or disrupt any information system or network infrastructure (data centers, servers, embedded systems, telephone systems, wiring closets, frame rooms, cable plant other than accessing designated outlets, etc.). Individuals found to be in violation of this prohibition may be subject to appropriate administrative sanctions, civil liability or criminal prosecution.
7. Protection of sensitive information. Individuals granted access to NSF/USAP information systems and services may, in the course of their official duties, have access to information designated by NSF as sensitive, or protected by federal law including, but not limited to, personal information, procurement information, trade secrets, and other information types. Individuals in such circumstances agree that the confidentiality, integrity, and availability of this information must be protected from unauthorized disclosure, loss, or corruption. Individuals found to be in violation of this prohibition may be subject to appropriate administrative sanctions, civil liability or criminal prosecution.

Limit of Access Authority

Permission to access or otherwise utilize NSF/USAP information systems and services shall be terminated upon separation from the United States Antarctic Program to include, but not limited to, termination of grant or grant extensions, termination of employment in support organizations, termination of Government employment, termination of guest/visitor status, determinations by NSF designated authorities to restrict or terminate access, etc. Continued use of NSF/USAP information systems and services, once access authority has terminated is a violation of federal law.

Acknowledgement

I, the undersigned, understand that I am authorized to access NSF/USAP information systems and services, as defined under the provisions of this Agreement. I acknowledge that I have received the required information security awareness briefing and my responsibility to abide by all information security policies, Rules of Behavior, procedures, and guidance issued by the National Science Foundation as applied to the United States Antarctic Program information systems and services, either directly or through its duly designated support organizations. I further acknowledge that I have read and understood the terms of this Agreement and agree to abide by them.

Printed Full Name:	Date:
Signature:	
Organizational Affiliation:	
Sponsoring Organization:	