

APPENDIX H: McMURDO STATION COMPUTER INFORMATION

For more information, visit <http://www.usap.gov/technology/contentHandler.cfm?id=94>

In this appendix, you will find information on the following:

- H.1 Information Security Awareness User Information Booklet
- H.2 Information Security Computer Screening Requirements
- H.3 Acknowledgment of Information Security Policies

H.1 INFORMATION SECURITY AWARENESS USER INFORMATION BOOKLET

Please familiarize yourself with information contained in the Information Security Awareness User Information Booklet at: <http://www.usap.gov/technology/documents/RSPC-05-500.pdf> or as provided by RSPC in U.S. participant medical kits or electronic grantpacks.

The information provided at the link above is extremely important. Please feel free to download for use.

NOTE: U.S. Participants **MUST** sign and return computer form located on the last page in the Information Security Awareness User Information Booklet; Non-U.S. Participants will receive form from the SMO. Non-U.S. Science Team Members are required to sign and return the computer form to the SMO intending to use the USAP network or USAP computers. Please contact the SMO if you have any questions or concerns.

H.2 INFORMATION SECURITY COMPUTER SCREENING REQUIREMENTS



United States Antarctic Program Information Security Computer Screening Requirements

Raytheon
Polar Services

The U.S. Federal government requires security and operational practices for computing systems in all government funded programs. The United States Antarctic Program's (USAP) compliance with this federal requirement entails the screening of all computers prior to connecting to the USAP network (wired or wireless). The following requirements apply to personal and business equipment that will connect to the USAP network.

See detailed information below regarding system requirements, operating system specifications, and the process for computer screening. The following requirements are aligned with the *NSF Computer Security Policy*. Please direct inquiries to the USAP Help Desk at (720) 568-2001 or helpdesk@usap.gov.

In order to minimize wait time for computer screening, please ensure your system meets the following requirements prior to deployment. Failure to comply with the following guidelines may result in excessive delays or a denial of access. Please be prepared.

General System Requirements

► Administrator Access

Obtain Administrator password for personal computers prior to deployment. Technicians must have the authority to log on to the personal computers at an Administrator level. This enables the screener to accurately review the system configuration and install any necessary patches and antivirus definition files, run screening software, and make any system configuration modifications necessary to provide network connectivity. If an Administrator password is not available, the screening process, as well as the ability to connect to the USAP network and its resources, will be delayed.

► Connectivity

All the equipment necessary to connect the computer system to a network must be provided, including the NIC (network interface card), external dongles or attachments used by the NIC, device drivers, etc. All equipment must be in working order.

► Antivirus

Administrator ID and password are needed for the antivirus software to update current virus definition files (DAT files). For computers running McAfee antivirus software, the Admin ID and password are needed to configure the software to update automatically from a local USAP server. Raytheon Polar Services Company (RPSC) can provide current DAT files for McAfee and Norton users. All other antivirus software users must ensure proper updates are installed and the computer is virus free prior to deployment. Please note that antivirus software requirements do not apply to computers running a Mac OS X or Linux operating system.

► Patches

Computers running Microsoft Windows operating systems must have the ability to be "patched" and include the most current level of the operating system.

► Client and Server Software

- Client software used for the purposes of email and web browsing, and other client software, such as SSH and SFTP, are permitted.
- Peer-to-peer (P2P) software, e.g., KaZaA, is not allowed.
- Email server software that provides SMTP/POP port services should not be used.
- Web server software that provides HTTP/HTTPS/FTP services should not be utilized.
- Network management servers, such as DNS and SNMP, should not be running.

Operating System Specifications

Operating systems have certain criteria that must be met in order to pass the computer screening process. All operating systems should utilize software supported by the operating system vendor. If a user's OS is not in one of the below categories, their connection to the network must be evaluated at a USAP location by an IT technician prior to connecting to the USAP network.

► Apple

Mac OS X systems are permitted to connect to the USAP infrastructure at any station. If older Mac OS versions are installed, current antivirus software must also be installed.

► Linux

Linux systems/partitions are permitted to connect to the USAP infrastructure at any station. If the computer is configured to dual boot with Microsoft, the Windows partition must comply with the criteria stated below for Microsoft systems.

► Microsoft

Ensure the following conditions are met:

- Windows 2000 (Service Pack 4) or XP (SP1 or SP2) and all hot fixes loaded*
- Current antivirus software with latest virus definition files (DAT files)
- Complete/full system virus scan within the previous two weeks
- System32/wins folder does not contain "dllhosts.exe" or "svchosts.exe"

*Microsoft OS service pack and security patch updates are available at www.microsoft.com

Computer Screening Process

Screening technicians will gather various computer information (see table below), and make it available to all technicians performing screenings on station. Users found using the USAP network without a screening rating of Pass are in violation of IT Security Policy and may be subject to disciplinary action. If possible, computers will be screened during Deployment Orientation for current antivirus software and operating system patches.

► Deployment Orientation or Christchurch, New Zealand

Computer screenings during Deployment Orientation or in Christchurch may take anywhere from two hours to a full day. Computers that receive a Pass rating at Orientation/Christchurch within two weeks of deployment may connect to the USAP network upon arrival. A Fail rating indicates the computer must go through remediation before connecting to the USAP network.

► McMurdo Station or South Pole Station

Computer screening in McMurdo or South Pole is not required for those computers that have received a Pass rating when screened at other USAP locations within two weeks of deployment. If a computer arrives on station either without being screened or having failed a screening, the owner must contact the McMurdo or South Pole Station Help Desk. IT personnel at McMurdo or South Pole will then perform screening and/or remediation as time allows.

► Marine Research Vessels (LMG or NBP)

Screening onboard the Vessels will occur during the port call or within the first two days at sea. IT personnel will perform screening and/or remediation as time allows. Laptops will be returned to their respective owners within 1-2 days.

► Palmer Station

Computers arriving at Palmer Station are required to be screened and configured for proper connection to the USAP network. Owners must contact Palmer Station IT personnel prior to connecting to the network. IT personnel will perform screening and/or remediation as time allows.

Data Potentially Collected During Computer Screening	
<ul style="list-style-type: none"> ▪ User name ▪ Date of check ▪ Computer make and model ▪ Computer affiliation (personal, grantee, NSF, other) ▪ NSF Tag number (if applicable) ▪ Computer hostname ▪ OS version ▪ OS patch level 	<ul style="list-style-type: none"> ▪ Service pack/service release level ▪ Serial number ▪ MAC address ▪ Wireless MAC address ▪ Antivirus software ▪ Virus DAT file date ▪ Pass (computer cleared to connect to network) or Fail (computer needs remediation)

H.3 National Science Foundation Acknowledgment of Information Security Policies and Permission for Use of NSF/USAP Information Systems and Services

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.

Page 1 of 2

NSF/OPP Information Security Acknowledgement
United States Antarctic Program
September 9, 2005

_____/_____
Initials Date

(over)

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:	