



United States Antarctic Program Information Security Awareness

User Information Booklet

Prepared for the National Science Foundation / Office of Polar Programs
by
Raytheon Polar Services Company
7400 South Tucson Way
Centennial, CO 80112

RPSC-05-500
Release 3.0

Posted 01/23/2006

Welcome to the United States Antarctic Program (USAP),

This booklet includes a summary of the USAP Information Security Awareness Program and a copy of the USAP Enterprise Rules of Behavior (EntROB) that govern personal behavior when using USAP information systems.

In accordance with Federal law, the National Science Foundation (NSF) is required to ensure that all USAP participants receive, understand, and acknowledge training on USAP policies related to Information Security. This material is designed to meet these requirements while providing you the required information in a succinct format to maximize the efficient use of your time while in the USAP.

For more detailed information, USAP-specific policies and guidelines can be reviewed by visiting the Information Security section within the USAP website (<http://www.usap.gov/technology>).

If you have any questions about the enclosed information, or desire additional copies of the booklet, please contact the USAP Help Desk at 720-568-2001 or helpdesk@usap.gov.

Thank you for your participation.

National Science Foundation
Office of Polar Programs



NSF Perspective on Information Security

Telecommunications and network access at all USAP stations is provided by the National Science Foundation (NSF), an agency of the United States Federal Government.

As a government agency, NSF's Information Systems Security Program must comply with all applicable laws, OMB circulars, Presidential Decisions Directives, and other regulations and guidance related to Federal Information Systems security. A key requirement is ensuring that NSF's Information Systems Security Program complies with all Federal Information Security Management Act (FISMA) requirements.

FISMA requires an agency implement an agency-wide information security program that includes "security awareness training to inform personnel, including contractors and other users of information systems that support operations and assets of the agency, of information security risks associated with their activities; and their responsibilities in complying with agency policies and procedures designed to reduce these risks."¹

This Information Systems Security briefing is designed to meet the FISMA requirement for users of National Science Foundation information systems.

¹ Section 301 FISMA 3544 (b) (4)



Why Is Information Security Awareness Important?

The United States Federal government requires mandatory periodic security awareness briefings for all Federal Information Technology (IT) system users, including contractor personnel, military personnel, and science grantees.

Information Security is a responsibility of and affects all users of the USAP infrastructure, not just the IT staff. Annual awareness briefings, supplemented by periodic reminders, keep all users cognizant of major security issues.

What is Information Security?

Information Security is much more than keeping hackers and viruses out of your computer. There are three key elements of Information Security known as the Information Security Triad:

Element	Focus	Example
Confidentiality	Ensuring information is protected from unauthorized access or disclosure.	Privacy Act and medical information collected when participants go through medical screenings for deployment.
Integrity	Ensuring information is protected from being changed inadvertently or by unauthorized individuals.	Science grant information collected to support a grantee on the Ice.
Availability	Ensuring information resources are protected so they can be utilized when needed.	Fully operational email and ensured availability of bandwidth.



What is your role in Information Security?

As a user of USAP IT resources, you play a critical role in ensuring that information resources are protected to meet the elements of the Information Security Triad. During your day-to-day operations, you can best meet these duties by doing the following:

- *Be proactive:* Adopt good security best practices as described later in this booklet.
- *Be a learner:* Understand security threats that affect your environment.
- *Seek help and advice:* Utilize Information Security representatives to fully understand how you can help maintain a secure environment.
- *Report Incidents:* Immediately report actual or suspected information security incidents, or any incidents of suspected fraud, waste, or misuse to your local on-ice or vessel IT support function, or the USAP Help Desk at helpdesk@usap.gov and 720-568-2001. The USAP Help Desk will forward it to the appropriate information security staff.

REMEMBER

A security program is only as strong as its weakest link.



Threats to Information Resources

There are many types of information resources that Information Security practices are designed to protect. Some of these resources include bandwidth, medical records and reports, as well as science and personal information. The threats to these resources are very diverse.

What threats does Information Security protect against?

Information Security protects against internal and external threats.

Internal Threats	External Threats
<ul style="list-style-type: none">▪ Accidental / intentional loss or change of data▪ Fraud, waste and abuse▪ Disgruntled users▪ Unethical behavior	<ul style="list-style-type: none">▪ Natural disasters (flood, storm damage, fire)▪ Criminal events (robbery, arson)▪ Information-focused attacks (hackers)

Besides hacking, how are threats manifested?

You should be aware that external threats can take on methods much more cunning than pure network or computer hacking. Today there are increasing reports of identity theft, phishing, and social engineering. Each of these threats is defined below:

Threat	Focus	Example
Identity Theft	Theft of identity information that could be used to compromise personal financial resources (bank accounts, credit cards, stock brokerage accounts, etc).	Spyware loaded on a user's computer that captures a user's SSN or bank account number transaction.
Phishing	The act of sending an email to a user and falsely claiming to be an established legitimate enterprise in an attempt to deceive the user into surrendering private information that will be used for identity theft.	Email imitating the appearance of an official email from the user's bank and asking the user to verify his account information by clicking on the URL provided in the email.
Social Engineering	The acquisition of sensitive information or inappropriate access privileges by an outsider, based upon the building of an inappropriate trust relationship with insiders.	A user getting a phone call from someone representing themselves as calling from the local IT department and asking for the user to provide his password in order to conduct a test.



Acceptable Uses of USAP Resources

USAP Policy 5000.6, *Acceptable Use of USAP Information Resources*, provides guidance on acceptable and prohibited uses of USAP resources and should be referred to when determining if a practice is acceptable or prohibited.

What are the acceptable uses of USAP IT resources?

The following list includes examples of acceptable uses of USAP resources. All uses are subject to risk assessments and NSF rules.

- **Personal email** – Not to interfere with mission.
- **Personal Internet** – Not to interfere with mission.
- **Recreational web browsing** – Not to interfere with mission; no downloads of prohibited material.
- **Instant messaging** – Not to interfere with mission and subject to controls to prevent bandwidth congestion and the introduction of harmful viruses.
- **Personal encryption** – Users may employ available encryption methods at their own expense on their non-USAP system when using the government's information infrastructure. Encrypted communications are still subject to monitoring and other authorized auditing actions. As a condition of use, users may be required to surrender their encryption key to appropriate NSF or law enforcement officials to assist in authorized investigative activities.
- **Third party software** – Subject to management approval, users may install third party software, including freeware and shareware, when the software is required to support their work responsibilities. Users must possess a valid license for all third party software installed on government information systems assigned for their use. Prior to installation, users must use antivirus tools to ensure the software is free of viruses. If the third party software is discovered to be the cause of system errors or other problems, it will be removed.
- **Personal business** such as online banking, shopping, etc. that does not interfere with mission.



Prohibited Uses of USAP Resources

What are the prohibited uses of USAP IT resources?

Users **will not** engage in prohibited activities. Network and share drives are monitored for violations. IT Station Managers have the authority to further restrict non-mission activities that have an impact on the infrastructure. Prohibited activities include:

- **No illegal activities**
- **No activities that can harm the infrastructure**
- **No classified information**
- **No downloading pornographic, sexist, racist or threatening material**
- **No email chains or email broadcasts**
- **No personal servers for email, web, ftp, telnet, or similar applications. All servers, science project or operational program participants, must be in Research Support Plan and/or be approved by established USAP Configuration Management processes and the NSF**
- **No chat room or newsgroup hosting inside USAP network**
- **No political campaigning**
- **No network gaming activities**
- **No hosting of personal e-commerce or non-program business activities**
- **No network monitoring tools**
- **No unauthorized wireless access points**
 - **Wireless access points, wireless routers, switches/hubs, and other network infrastructure are not authorized for personal use.**
 - **Wireless access points, wireless routers, switches/hubs and other network infrastructure for official business use must be approved by established Configuration Management processes and the NSF.**
- **No violation of U.S. or international copyright laws, particularly digital media**
- **No peer-to-peer (P2P) applications, unless it is essential for official business purposes and has been approved by USAP Configuration Management processes and the NSF**



Why Peer-To-Peer Applications Are Prohibited

What is Peer-To-Peer (P2P)?

Peer-To-Peer (P2P) is a method of exchanging files between computers without the use of a centralized server. P2P allows users who want access to files and information to interact directly with each other and to share information without the intervention of a server. It is commonly used to anonymously exchange media and software. Examples include KaZaA, BearShare, LimeWire, and Morpheus.

What are the dangers and risks of P2P?

Peer-To-Peer undermines network security by circumventing firewalls, intrusion detection systems, and perimeter-based antivirus software. Certain NSF systems are allowed to use P2P but *only* under controlled and approved configurations.

Specific risks associated with P2P include:

- High bandwidth consumption
- Lawsuits by Recording Industry Association of America (RIAA), Business Software Alliance, etc. over copyright violations
- Copying and sharing of inappropriate or copyrighted material
- Viruses, SpyWare, Trojan horses

What is not P2P?

Instant Messaging (e.g., MSN Messenger, AOL Instant Messenger) and Group meeting software (e.g., WebEx, Centra, MS NetMeeting) are **not** considered P2P.

What should I do if P2P applications are installed on my computer?

P2P applications are difficult to remove, as they modify registry values and have many associated "adware" programs. Local IT technicians at USAP locations will assist with removal of P2P applications and can be requested by sending an email to helpdesk@usap.gov.



Copyright Infringement

Federal law prohibits the unauthorized copying, sharing, or distribution of copyrighted materials (music, video, software, etc.) and these activities are strictly prohibited on USAP resources.

What are examples of strictly prohibited activities?

Strictly prohibited activities include:

- Illegal MP3 copying, sharing, or distribution
- Illegal DVD copying, sharing, or distribution
- Illegal video copying, sharing, or distribution
- Illegal music CD copying, sharing, or distribution
- Illegal software copying, sharing, or distribution

This policy is not intended to prohibit the legal purchasing of music or video entertainment (within bandwidth restrictions).

Am I accountable if I conduct these activities?

In the past, some USAP participants have illegally copied, shared, or distributed music, video, software, etc. using USAP IT resources. This will not be tolerated, and persons found in violation of federal and international copyright laws will be held accountable. *USAP network and share drives are periodically monitored for violations.*

By signing the *NSF/OPP Information Security Acknowledgement* form and accepting the USAP network logon, you acknowledge your accountability to comply with copyright laws. The Enterprise Rules of Behavior (EntROB) also require that all copyright laws must be followed while using USAP infrastructure or equipment.

WARNING Violation of copyright laws will not be tolerated.



An Important Note on Bandwidth Usage

Bandwidth is an extremely scarce and expensive resource at each of the USAP stations in Antarctica.

The prohibitions listed above are intended to ensure bandwidth is available for scientific uses and is not congested with inappropriate activities.

Please note that at certain times approved applications may also cause bandwidth congestion, and users may be required to limit their activities if bandwidth congestion becomes an issue.





General USAP IT Best Practices

Password Protection

Protection of your personal password constitutes an important “first layer” in the total Information Security protection architecture.

Password requirements include:

- Minimum of eight alphanumeric characters in length
- Does not contain your account or full name
- Expires every 90 days and not reused for one year

Password/Pass-phrase Tips:

- Change password regularly
- Use strong passwords (8 characters, mixed-case, special characters)
- Make it easy to remember and hard to guess
- Protect your password – DO NOT share passwords or write it down
- Examples of strong passwords include:
 - “D@rkg066Le\$” (Dark goggles)
 - “th1Kpant\$ (Thick pants)

It is also important to ensure an operating system is installed that provides password protection capabilities. For example, Windows 95/98/ME do not provide password protection.

Antivirus Protection

To provide protection from malicious code, all computers connected to the USAP network are required to have some form of active and up-to-date antivirus software in operation. All participants must ensure that the antivirus definition files are kept current, preferably by enabling the auto-update function.

There may be rare exceptions to this policy such as when grantee instrumentation computer system software may be incompatible with anti-viral software. These systems should be identified in the Research Support Plan.

IT technicians at operating USAP locations can provide antivirus updates for McAfee and Norton users. All other antivirus software users must ensure proper updates are installed prior to deployment.

It is also important to ensure all patches for operating system and software applications are up-to-date prior to deployment.



General USAP IT Best Practices (continued)

Physical Security

Theft of laptops is a recurring threat, especially while traveling. Always maintain physical contact with your laptop, PDA, etc. and never check-in a laptop, PDA, etc. with luggage.

Report loss or theft of any computer equipment, personal or US Government, as soon as possible to a local IT specialist and/or IT Help Desk.

Encryption of Personal Communications

Users may employ available encryption methods at their own expense on their non-USAP system when using the government's information infrastructure. Encrypted communications are still subject to monitoring and other authorized auditing actions. As a condition of use, users may be required to surrender their encryption key to appropriate NSF or law enforcement officials to assist in authorized investigative activities.

Protect Your System from Unsolicited Email

Unsolicited or unwanted email is sometimes referred to as "SPAM" or electronic junk mail. The following tips are recommended steps in protecting your system from SPAM:

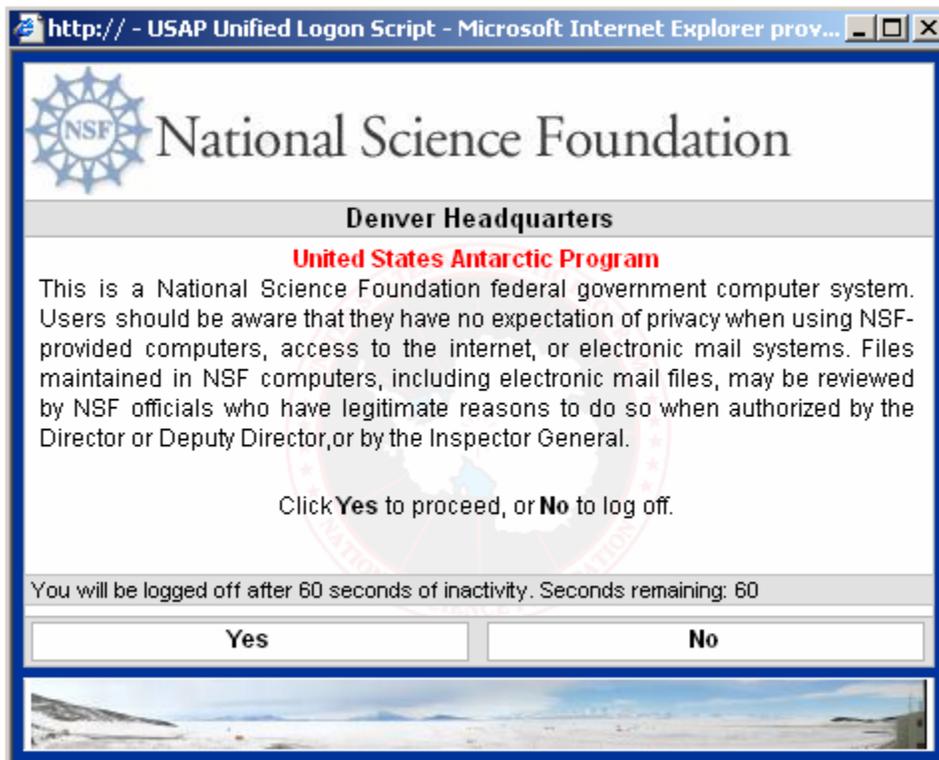
- Never respond or try to "unsubscribe"
- Never send a "flame" response
- Delete, without review, all suspicious or unexpected email traffic
- Forward SPAM email to SPAMSuspect@usap.gov



Expectation of Privacy

The USAP Logon Banner is displayed on all USAP information systems within the USAP infrastructure. The deployment and display of this banner brought USAP into compliance with Federal and NSF directives.

It is important that users read and understand this banner and are aware that they have no expectation of privacy when using NSF owned or provided information systems, which includes computers and access to the internet. Monitoring of USAP resources does occur in order to maintain the proper operational, maintenance, and security posture of the enterprise information systems.



NSF provided email systems (i.e., the Microsoft Exchange mail service and local LAN Microsoft Outlook mail client mail stores) are the property of the US Government and NSF. If users prefer to not have their personal communications subject to the NSF disclosure policy (described above and on the NSF Security Acknowledgement Form), then users should use their own web-based mail service and avoid storing their messages on the USAP network or desktop storage systems.



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

Information System Rules of Behavior USAP Enterprise Information Infrastructure

EFFECTIVE DATE: 1 AUGUST 2004

1. ACCEPTABLE USES OF USAP INFORMATION RESOURCES

The following activities are considered acceptable uses of the USAP Information Infrastructure. All users are reminded that USAP mission activities always take precedence over any personal activity. The NSF reserves the right to restrict or otherwise limit personal use based on resource availability, conflict with official business, and unacceptable information security risks.

Personal Telephone and Facsimile Use. Users may make personal telephone calls (including use of facsimile machines and voice mail), provided such use complies with these Rules and other USAP policies and procedures, and involves only a minimal cost to the government. The user is responsible for charges incurred when using the infrastructure for personal use.

Personal Use of Electronic Mail. Some limited personal use of the government's electronic mail services is permitted, provided it does not interfere with the participant's work or the work of others. Typical authorized limited personal use of email includes emergency communications and personal communications with family members, health care professionals, or teachers.

Personal Use of the Internet. Some limited personal use of Internet services is permitted, provided it does not interfere with the participant's work or the work of others. Extreme care must be taken regarding content matter. Typical authorized limited personal Internet use includes:

- Accessing travel information, forms or information on the Intranet or Internet
- Accessing parent organization information and online resources
- Accessing state and local government agencies on personal matters etc.
- Work-related events, such as technical symposiums, classes, and presentations
- Activities sponsored by the program, such as station recreational activities
- Events and activities specific to a particular USAP station or organization
- Program-sanctioned activities, such as blood drives, sanctioned clubs, and organizations
- Communications of reasonable duration using instant messaging applications
- Recreational web-browsing of a reasonable duration, during off-duty hours, that does not violate other elements of this policy and does not conflict with mission activities

Encryption of Personal Communications. Users may employ available encryption methods at their own expense on their non-USAP system when using the government's information infrastructure. Encrypted communications are still subject to monitoring and other authorized auditing actions. As a condition of use, users may be required to surrender their encryption key to appropriate NSF or law enforcement officials to assist in authorized investigative activities.

Third Party Software, Freeware and Shareware. Subject to management approval, users may install third party software, including freeware and shareware, when the software is required to support their work responsibilities. Users must possess a valid license for all third party software installed on government information systems assigned for their use. Prior to installation, users must use antivirus tools to ensure the software is free of viruses. If the third party software is discovered to be the cause of system errors or other problems, it will be removed.

Mailing Lists. Users are permitted to subscribe to mailing lists required to support their work responsibilities or grant tasks. While deployed to the Antarctic research stations or vessels, users must provide the local site

IT staff with appropriate unsubscribe information so the lists may be cancelled upon their departure. The NSF reserves the right to restrict or deny mailing list subscriptions and traffic to meet mission requirements. **Personal Business or Commercial Uses.** While deployed, users may conduct limited personal business matters using government information resources, such as when a sub-contractor needs to communicate with their home organization. Additionally, NSF may authorize the use of information resources to support the one-time disposal of personal items, such as normally occurs during the transition of personnel at the Antarctic research stations.

Election Material. It is acceptable to use the USAP information infrastructure to disseminate information regarding the process to participate in U.S. federal, state and local elections. For example, information about absentee ballot procedures is allowed. Information advocating a position for or against a candidate, an issue, or other element of an election is not allowed.

2. PROHIBITED USES OF USAP INFORMATION RESOURCES

The following activities are prohibited uses of the USAP Information Infrastructure.

Illegal Activities. All illegal activities are forbidden.

Adverse Activities. Any activity that could embarrass the NSF, adversely affect its interests, interfere with the performance of the USAP mission, or exceed allocated resources is prohibited.

No processing of classified information. The storage, processing or transmission of government classified information on unclassified computer systems, networks or via the Intranet and Internet is prohibited. All USAP information resources are to be considered unclassified and are not accredited for processing or transmitting classified information.

Hostile Environment. Under no circumstances is it permissible to access or download material that would create a hostile or offensive work environment, such as racist or sexually explicit material. This prohibition includes, but is not limited to, the following activities: accessing or transmitting sexual images, messages, jokes or cartoons; hate speech, or material that ridicules others on the basis of race, creed, religion, color, sex, disability, age, national origin, or sexual orientation or is otherwise defamatory or derogatory; content prohibited by law and/or regulation.

Prohibited Email Activities. Allowing others to use an assigned email account is prohibited. Placing others on a mailing list, subscription list, chat room list, or other list service without their consent is prohibited. Creating, originating, distributing or circulating "chain" or "pyramid" transmissions, mass mailings, hoaxes, or harassing messages is prohibited. "All employee" or broadcast messages disseminated using USAP information resources must be business related and approved in advance by the applicable manager. Using large distribution lists for non-business-related purposes, or sending large, memory intensive files or applications which may impede or disturb network operation is prohibited. Using email to proselytize or solicit for personal commercial ventures, religious or political causes, or outside organizations is prohibited.

Personal Information Services. Due to resource constraints, personal servers of any type are prohibited. In the case of approved science activities, all web services, file transfer services, and telnet/SSH services required for project support must be listed in the support requirements section of the user's science proposal, SIP, or ORW, and must be approved by NSF.

Chat Room and News Group Participation. Use of USAP information resources to participate in chat rooms, news groups, or similar activities where the public will view the posting is prohibited because such postings make use of the NSF's usap.gov domain. Use of the USAP Internet address of "usap.gov" is a representation of the National Science Foundation, analogous to the use of NSF letterhead in which the opinions expressed reflect on NSF.

Political Activities. Use of USAP information systems to support organized political activities, such as an election campaign or an organized lobbying activity is prohibited.

Gaming. Use of USAP information resources to participate in Internet-based gaming activities is prohibited due to the large consumption of bandwidth such activities incur. Gaming activities using local network resources may be permitted at the discretion of station managers.

Prohibited Business and Commercial uses. Conducting non-program business activities is prohibited. Using USAP resources to advertise commercial goods or services for sale for monetary or personal gain is prohibited.

Using USAP resources to conduct non-program commercial activities is prohibited. Users may not establish or maintain a web-based business at a USAP operating location.

Prohibited Network Activities. Knowingly downloading, installing, storing or using malicious software, viruses, "cracking," keystroke monitoring software, or other actions that may be disruptive or counter-productive to business operations is prohibited. The introduction or use of packet sniffing software or any software intended to capture passwords is prohibited except when explicitly authorized for contract or

business purposes and coordinated in advance with NSF. Monitoring network traffic (e.g., run a sniffer); accessing IT resources; or copying data, files, or software without prior authorization is prohibited

3. EXPECTATIONS OF PRIVACY WHILE USING USAP INFORMATION RESOURCES

Users of USAP information resources have no expectation of privacy with respect to any information residing on government information systems or transmitted over government information networks, other than the regular expectations associated with information governed by the Privacy Act of 1974, as amended. The NSF considers user information placed on USAP information systems or transmitted across the USAP information infrastructure to be entrusted information, which is not normally released for public viewing without the user's authorization.

The NSF will release user information found on USAP information resources to appropriate law enforcement agencies when asked to do so as part of an official investigation or other sanctioned activity. The NSF will, to the best of its ability, protect information within the USAP information infrastructure from unauthorized access. However, users make use of the government's information resources at their own risk. The NSF is not liable to the user for damages caused by unauthorized uses of the USAP infrastructure. Systems and Network administrators are authorized to access information located on USAP information resources or transmitted across the USAP information infrastructure when conducting their official duties. If such access occurs, the information will not be released for public viewing or to unauthorized persons.

4. GUIDING PRINCIPLES FOR THE USE OF USAP INFORMATION RESOURCES

In establishing these Rules of Behavior, the NSF has applied these guiding principles:

- USAP information resources, especially at the Antarctic research stations and aboard the research vessels, may be used for certain personal uses, in a manner that does not interfere with the program's mission. All mission activities take precedence over personal activities at all times.
- Personal communications, such as email or phone calls, that do not involve USAP business, will be considered entrusted communications, and not normally monitored or shared without the consent of the participating parties. Exceptions to this principle include requirements to make such communications available to support lawful investigations, to ensure proper operations and maintenance of the USAP infrastructure, or to correct or prevent damage to the USAP information infrastructure.
- Systems and network administrators, and others who may be exposed to a participant's personal communications as a part of their normal duties, are in a position of trust and will be held accountable for violations of that trust on their part.
- The National Science Foundation is not a common carrier, and does not possess the requisite infrastructure and resources necessary to guarantee the privacy of information processed or stored on USAP information systems or networks. Users of USAP systems agree that the government and its representatives are not responsible for the loss of personal information, or for the disclosure of personal information as a result of unauthorized activity by participants or by others outside the program.

Participants and their leaders are expected to use good judgment in appropriate use of program assets consistent with the purposes of these Rules. However, the final determination regarding what constitutes appropriate use consistent with these Rules is reserved to NSF management in coordination with the participant's organization.

5. ADDITIONAL GUIDANCE FOR USERS

User Responsibilities. When using the USAP information infrastructure you will be held accountable for your actions related to the information resources entrusted to you. USAP information resource users have the following responsibilities:

- Comply with these Rules of Behavior and all other USAP, OPP and NSF policies and procedures, as well as the policies and procedures of their sponsoring organization
- Protect sensitive information from disclosure to unauthorized individuals or groups. Disclosure of information is not at the users discretion, only when authorized by the NSF
- Ensure information security through effective use of user IDs and passwords
- Protect hardware, software, and information from damage, abuse, and unauthorized use
- Report security violations and vulnerabilities to the proper authorities. The Help Desk is the first point of contact for all reports
- Users shall not access, modify, duplicate, destroy, or disclose any information or software on a network or a computing system, unless so authorized
- Users shall not leave an active system unattended, thereby allowing an unauthorized person to gain access to a network or a computing system through the user's login session

- Users are responsible to ensure the integrity, availability, and confidentiality of all work-related data on systems assigned for their use. It is recommended that critical data on a hard disk be backed up periodically

Authorization for Access. Portions of the USAP information infrastructure are restricted to authorized users that have been granted special access permissions by the National Science Foundation or its authorized delegates. These areas are identified by warnings posted at their entry point or by the system's interactive request for authentication. You shall access only those areas for which you have been granted authorization to access.

Copyright and Intellectual Property Issues. All users of USAP information resources must comply with U.S. and international laws regarding copyrights and other intellectual property. Users must comply with copyright licenses associated with the USAP information resource they are using. Users shall not make copies of licensed software for other microcomputers users or personal use. The presentation or display of digital media such as software, pictures, literary works and songs must comply with existing laws.

Alternative Workplace. When working at home or an alternative workplace, USAP information resources users must establish security standards at their alternate workplace sufficient to protect hardware, software, and information. This includes having only those resources employees really need and have authority to use; establishing a thorough understanding and agreement with supervisors as to what employees' security responsibilities are; using software according to licensing agreements; ensuring that confidentially-sensitive information downloaded is secure; being alert for anomalies and vulnerabilities; and reporting these anomalies to proper officials and seeking advice when necessary.

Personal File Storage. Each user is typically assigned a 'home' directory on their primary network which is usually accessible from any computer. This drive is provided for the storage of personal files. Files stored in this directory are not considered private, but will be afforded some measure of confidentiality against unauthorized access and disclosure.

Common File Storage. At each operating location, one or more directories are established for common use, and are accessible to all users. A temporary directory is provided for temporary (less than one week) use by users. Users have full rights to this directory and may add or delete files and directories as needed. All files and directories in the temporary directory are deleted automatically once a week, on a schedule determined by the station IT staff. A permanent common area is intended for operational storage and use. Users typically have read-only rights to this directory.

Departmental File Storage. Within each station network, directories are established for the various functional departments and participant organizations. Management of the allocated space is the responsibility of that department, with the assistance of the contractor IT department. User privileges for their department directories are set at the discretion and with the approval of the department manager.

Laptop Computers and other portable devices. Laptops and other portable computing devices, such as Personal Digital Assistants, must be evaluated for compatible software and up-to-date antivirus protection before they are used on the USAP network.

Official Business. Official business broadly includes any information processing that is required as part of an individual's work responsibilities. Official business includes, but is not limited to, the performance of USAP work-related duties in position descriptions, professional training and class work, work covered under grant agreements with the NSF, tasks directed via NSF contracts, agreements with international partners, and support activities related to NSF contract tasking.

Ownership of Information. All information located on a government information system is the property of the government, unless otherwise identified as belonging to another entity as a result of a contract or a grant agreement with the government.

Personal Use. Personal use broadly includes any information processing that is conducted in support of activities that do not constitute official business. A personal use activity is typically one in which the individual user, or a non-USAP entity is the primary beneficiary. Participants who use program assets for personal purposes are responsible for any and all liability that may arise from such personal use to include any violation of law, regulation or policy during such use.

Use of Antivirus Applications. All users of USAP information resources must also comply with USAP policies regarding the use of antivirus software.

Sensitive Information. The USAP information infrastructure can be publicly accessed. Do not place any of the following types of information on a USAP information system unless you are specifically authorized or instructed to do so: Medical Information; Government Acquisition Information; Operational Security Information; Proprietary Information; any other information considered sensitive. Where applicable; USAP information resource users must acquire and use sensitive information only in accordance with established policies and procedures. This includes properly safeguarding sensitive information contained in hardcopy or

softcopy; and ensuring sensitive information is accurate, timely, complete, and relevant for the purpose which it is collected, provided, and used.

Reporting Violations. Users shall immediately report any known or suspected violations of these Rules or other Information Security policies or procedures. Please contact the USAP Help Desk at 720-568-2001 or helpdesk@usap.gov. Additional information may be found at <http://www.usap.gov>.

6. ADDITIONAL GUIDANCE FOR CONTENT PROVIDERS AND SYSTEMS ADMINISTRATORS

Auditing of Information Systems. Where applicable; system administrators or security administrators will regularly review telecommunications logs and phone records, and conduct spot-checks to determine if Users are complying with controls placed on the use of USAP information resources.

Protection of Personal Information. During the course of their duties, Content Providers and Systems Administrators may have access to information of a personal nature. This information is considered entrusted and is not to be disclosed unless authorized or directed to do so as part of a lawful investigation, or as directed by NSF management.

7. GUIDANCE ON PASSWORDS

Users shall follow the guidance below when creating or using their passwords:

- Passwords are considered operationally sensitive information and shall not be disclosed to co-workers; written down; or displayed anywhere that might allow others to copy or memorize them.
 - Users shall avoid using passwords containing obvious items or information, such as names, initials, important numbers, etc.
 - Passwords should not be trivial, predictable, or obvious.
 - Passwords should be at least eight characters long and should contain a combination of alphabetic (upper and lower case), numeric, and special characters. Never use all numeric passwords.
 - Avoid using words or permutations of words found in a dictionary.
 - Avoid using names of family members or pets, hobbies, dates, or other familiar or easily guessed information about yourself.
 - Change your password frequently (if the system(s) does not automatically.)
 - Passwords must be changed when they expire, or are compromised.
- Any unauthorized use of an account or improper distribution of a password may warrant the immediate termination of the account.

8. GENERAL INFORMATION

The National Science Foundation provides information systems for the purpose of transacting official business of the U.S. Antarctic Program. The NSF establishes Rules of Behavior for the proper use of these systems. Any non-program use of USAP information resources must be authorized by NSF management. The National Science Foundation has created these Rules of Behavior to guide users, content providers and system administrators in the appropriate and acceptable use of USAP information resources. This document applies to all information resources that comprise the USAP Enterprise information infrastructure and to all users of these information resources. In this document, the term "you" or "your" refers to the User. The term "User" also includes Content Providers and Systems Administrators.

The USAP information infrastructure is a federal government information system composed of several interrelated information systems owned by, and operated for, the National Science Foundation. A significant portion of USAP program activities take place at remote or isolated locations managed by the U.S. government. Private sector support infrastructure is not available for the personal use of program participants at these locations. Consistent with federal guidelines for agency management of agency resources (5 USC 1103(a)(3)), USAP information systems may be used for morale and welfare purposes as deemed appropriate by program management.

Information maintained in NSF systems, including electronic mail files, may be reviewed by NSF officials who have a legitimate reason to do so when authorized by the Director or Deputy Director, or by the Inspector General. Unauthorized attempts to modify any information stored on this system, to defeat or circumvent security features, or to use this system for other than its intended purposes are illegal and may result in disciplinary action, criminal prosecution, or both.

Where applicable; USAP information resource users must comply with NSF policies and procedures, as well as your own organization's policies and procedures governing the personal use of NSF government

equipment. In the event of a conflict, the NSF policies and procedures, including these Rules of Behavior, take precedence. NSF specific policies and guidelines can be reviewed by going to the NSF web site (<http://www.nsf.gov/>) and selecting "Policies."

These Rules of Behavior apply to all users of the USAP information infrastructure whether you are an NSF employee or not. USAP information resource users must comply with these Rules of Behavior. Because written guidance cannot cover every contingency, you are asked to go beyond the stated rules, using your best judgment and highest ethical standards to guide your actions. These Rules are based on Federal laws and regulations and agency directives. As such, there are consequences for non-compliance. Depending on the severity of the violation, at the discretion of management and through due process of the law, consequences can include: suspension of access privileges, reprimand, suspension, demotion, removal (dismissal), and criminal and civil penalties.

Your acknowledgement of these Rules of Behavior and your continued use of the system constitute your acceptance of these Rules of Behavior and of other relevant rules and regulations of the federal government and the National Science Foundation. Acknowledgement is accomplished by selecting the agreement button when prompted to do so, or by signing a copy of this document as part of your account processing.

If you have any questions about these Rules, please contact the USAP Help Desk at 720-568-2001 or helpdesk@usap.gov. The responsible NSF point of contact for these Rules of Behavior is Mr. Patrick D. Smith, NSF Office of Polar Programs, 4201 Wilson Blvd, Suite 755, Arlington, VA 22230, 703.292.8032. NSF specific policies and guidelines can be reviewed by going to the NSF web site (<http://www.nsf.gov/>) and selecting "Policies."

9. ACKNOWLEDGEMENT OF THESE RULES OF BEHAVIOR

Your acknowledgement of these Rules of Behavior and your continued use of the system constitute your acceptance of these Rules of Behavior and of other relevant rules and regulations of the federal government and the National Science Foundation. Clicking "Yes" in the USAP Logon prompt is an indication of your acknowledgement and acceptance of the EntROB.

Required Action for Acknowledgement

Sign and return the *NSF/OPP Information Security Acknowledgement* form to acknowledge the Enterprise Rules of Behavior (EntROB) and Information Security Awareness Program.