



United States Antarctic Program Information Security Awareness

User Information Booklet

Prepared for the National Science Foundation / Office of Polar Programs

Raytheon Polar Services
7400 South Tucson Way
Centennial, CO 80112

RPSC-05-500
Version 3.0

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 to 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 booklet 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 training, 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:

- *Being proactive:* Adopt good security best practices as described later in this booklet.
- *Being a learner:* Understand security threats that affect your environment.
- *Seeking help and advice:* Utilize information security staff to fully understand how you can help maintain a secure environment.
- *Reporting 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 can be very diverse, and include both 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** –Personal business such as online banking, shopping, etc. that does not interfere with mission. Note that excessive downloading of purchased material (iTunes®, etc.) creates bandwidth congestion and interferes with the 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 do not interfere with mission.

For more information on acceptable uses of USAP resources, please read the Information System Rules of Behavior located on the USAP website at <http://www.usap.gov/technology/documents/EntROB.pdf>



Prohibited Uses of USAP Resources

What are the prohibited uses of USAP IT resources?

In order to protect information resources and abide by U.S. law, some activities (emphasized below) are prohibited. 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
- Activities that can harm the infrastructure
- Classified information
- Downloading pornographic, sexist, racist or threatening material
- Email chains or email broadcasts
- 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
- Chat room or newsgroup hosting inside USAP network
- Political campaigning
- Network gaming activities
- Hosting of personal e-commerce or non-program business activities
- Network monitoring tools
- 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.
- 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
- Excessive downloading of data (music files from iTunes®, etc.) and streaming media are prohibited.
- Use of non-USAP supported Voice-over Internet Protocol (VoIP) software (Skype™, etc.) is prohibited.

For more information on prohibited uses of USAP resources, please read the Information System Rules of Behavior located on the USAP website at <http://www.usap.gov/technology/documents/EntROB.pdf>



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. P2P applications are commonly used to anonymously exchange media and software.

Examples:

- Skype™
- ©Sharman Networks KaZaA
- BearShare®
- ©Lime Ware LLC., LimeWire
- Morpheus™

It is against NSF-agency policy to use P2P applications unless specifically authorized for legitimate official business purposes.

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

What are examples of copyrighted material?

- MP3, WAV, or other audio files
- Digital video files
- DVDs or music CDs
- software programs

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.



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 twelve alphanumeric characters in length
- Does not contain three or more consecutive characters from your username.
- Contains characters from at least three of the following four categories:
 - English uppercase characters (A - Z)
 - English lowercase characters (a - z)
 - Base 10 digits (0 - 9)
 - Non-alphanumeric (For example: !, \$, #, or %)
- Expires every 60 days and not reused for one year

Password/Pass-phrase Tips:

- Change password regularly
- Use strong passwords (12 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), "Tr@vel2Ant@rctica" (Travel to Antarctica)

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 antivirus 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 visual or 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 U.S. 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:

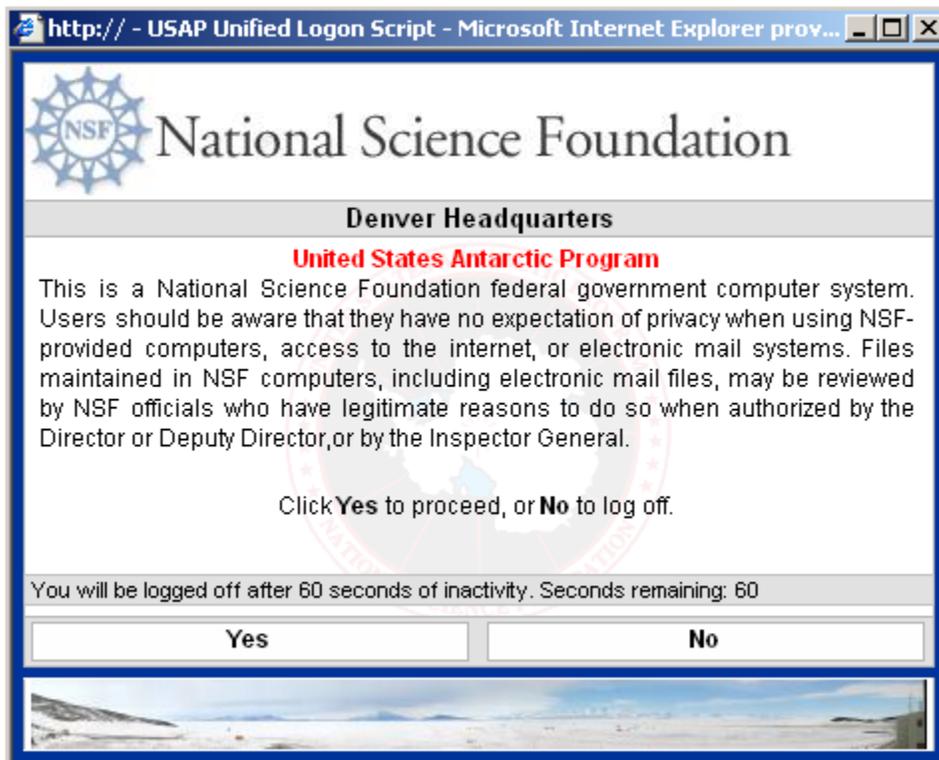
- Never respond or try to "unsubscribe"
- Never send a "flame" response
- Delete, without review, all suspicious or unexpected email traffic
- Forward SPAM email to SPAMSuspect@usap.gov



Expectation of Privacy

The USAP logon banner is displayed on all USAP information systems within the USAP infrastructure. The use of this banner ensures USAP 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.



Bandwidth

Internet bandwidth is a valuable commodity in the USAP. Basic operations of the USAP and support for science are dependent on the satellite communications that support Internet availability to USAP operating locations. Due to limited bandwidth available on station, at times personal use of the Internet can have staggering impacts on the USAP network.

For example, bandwidth available at McMurdo station is equivalent to the amount available to one household serviced by a cable modem. For a single family household, these resources are typically sufficient for performing any activity on the Internet. However during the summer season at McMurdo station when over 1,000 people are sharing this resource, it is essential that available bandwidth is primarily dedicated to operational and science support requirements. Some USAP operational uses of bandwidth include support for direct-dial telephone service to the U.S., mission critical operations applications, and support for emergency telemedicine.

Remember that when using the Internet while on the USAP network, any personal use of the Internet is secondary to support of basic operations of the program, and to the generation and support of scientific data.

The USAP Enterprise Rules of Behavior list acceptable and prohibited uses of USAP resources; however, acceptable use can be limited or restricted if necessary to support mission-critical work.

If you are found abusing the privilege of using the USAP network for morale or personal purposes, you will be notified. Upon further abuse, your supervisor will be notified, and your use of the network may be restricted or prohibited. Please use the USAP network wisely and courteously. If you have a question about what may or may not impact the USAP mission, please contact the Denver Headquarters IT Help Desk, and they will be happy to help you.

Additionally, for those of you who are using the network for authorized official use, such as for grantee data transfer of scientific data to your home institution, you must adhere to your approved levels of service. It is important that all network use is coordinated through the USAP to ensure that all groups receive access to appropriate resource levels, and more importantly to ensure that essential operations of stations is not impacted by other network activities.

If your work requires changes to your authorized level of service, be sure to receive approval for this change before changing your network use practices. If your network activities exceed your authorized level of service you will be notified, and if necessary your usage of the network may be restricted or prohibited.



Personally Identifiable Information (PII)

Personally Identifiable Information (PII) is information about an individual maintained by an agency which can be used to distinguish or trace an individual's identity. PII is typically a combination of two or more of the following identifiers; name, social security number (SSN), date and place of birth, mother's maiden name, biometric records, educational history, financial transactions, medical history, criminal history and employment history.

Why is protecting PII important?

- To protect all USAP participants from release of personal data and potential identity theft.
- To ensure the USAP complies with NSF regulatory requirements.

All USAP participants are responsible for recognizing sensitive information and avoiding inappropriate access, use, or disclosure.

To avoid unauthorized disclosure of PII, follow best practices for handling sensitive information:

- Only use systems, software, and data for which you have authorization, and only use for official government USAP business.
- If you have access to systems and data that utilize PII, specifically SSNs, view and access this information only for the purposes for which use of the data is intended.
- Store records containing sensitive information on network drives with access limited to those individuals or entities that require access to perform a legitimate function.
- Secure all removable or transportable media (e.g., paper forms, reports, cassettes, CDs, USB drives, etc.) containing sensitive information when not in use. Security measures may include locked file rooms, desks, cabinets and encryption.
- When no longer required, destroy or dispose of paper documents and electronic media containing sensitive information using methods designed to prevent subsequent use or recovery of information.
- Do not transmit SSNs via email.
- Only transmit PII via email if the data is encrypted.
- For storage or transmission purposes, do not store sensitive information on portable devices such as laptops, PDAs and USB drives or on remote/home systems unless you have written authorization and the portable device/data is encrypted.



PII Disclosure Incident Response

The unauthorized disclosure of PII is when an individual gains logical or physical access without permission to USAP network, system, application, data, paperwork, or other resource that results in the unauthorized release ("spill") of personally identifiable information (PII). Examples include:

- Intentional unauthorized access to PII.
- Loss of a USAP portable device containing PII.
- Loss of paper documents containing PII.

In the case of suspected or actual unauthorized access or disclosure of sensitive information, report the incident immediately to USAP Denver Headquarters:

HelpDesk@usap.gov
720.568.2001 direct
800.688.8606 ext. 32001

Federal reporting timeframe: immediately but no later than within one hour of discovery/detection.