National Science Foundation

United States Antarctic Program (USAP)

FY15 Information Security and Privacy/Sensitive Information Awareness Training

Contents

Training Goals

The goals of this course are:

- To make you aware of threats to USAP information resources and privacy/sensitive information and your responsibilities for their protection.
- To familiarize you with USAP policy on network usage
- To promote a working knowledge of accepted and prohibited usage of the USAP network
- To familiarize you with methods for handling privacy and sensitive information
- To tell you what to do in the event of a loss or breach of information

Why Security and Privacy Awareness Training?

Security and Privacy Awareness training is mandated by the Federal Information Security Management Act (FISMA).

The cyber frontier is a dangerously shifting landscape with new and emerging threats. The NSF seeks to maintain the USAP network as an **open and collaborative** working environment while ensuring that its systems and information are secure. While threats continue to grow in number and sophistication, there are many layers of controls in place to protect USAP systems and assets and **you** are one of them.

What Is Information Security?

In a nutshell:

Information security is protecting information (print, electronic, or any other form) and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction.

There are three main goals of IT security:

- **Confidentiality,** where sensitive information is protected from unauthorized disclosure.
- **Integrity**, which means electronic information is not corrupted, and
- **Availability**, which means information is available when needed

Why Is Information Security Important?

The USAP mission depends on information systems that operate continuously, maintain a high availability, and ensure information is protected from unauthorized disclosure. Misuse of USAP resources can put the USAP mission at jeopardy.

- Your everyday actions either support our security posture or they make us vulnerable.
- Secure practices are not a choice - they are a **necessity**.
- Key awareness themes continue to be:

- Protect sensitive information, including proprietary information and personally identifiable information, or PII.

- Recognize and avoid social engineering ploys that try to trick you into giving up personal information and clicking on email attachments or Internet links that could infect your computer with malicious software.

- Recognize that **you are responsible** for protecting the information you use everyday.

Why Do I Care?

- Use of USAP information technology resources is a **privilege** that can be withdrawn if you do not comply with the secure operating practices required.

- Failure to exercise your information security responsibilities can subject you to civil liability or criminal prosecution.

Your Responsibilities

Know the information security risks associated with your use of USAP information technology resources and be familiar with the defenses and protections needed to manage the risks.

Understand that your use of USAP information technology resources is a privilege that can be withdrawn if you do not comply with the secure operating practices required.

It Is **Your** Responsibility to:

- Protect Sensitive Information from disclosure.
- Ensure information security through the use of user IDs and strong passwords.
- Protect hardware, software, and data from damage, abuse, and unauthorized use.

<u>You are responsible for protecting the Government data on your computer.</u>

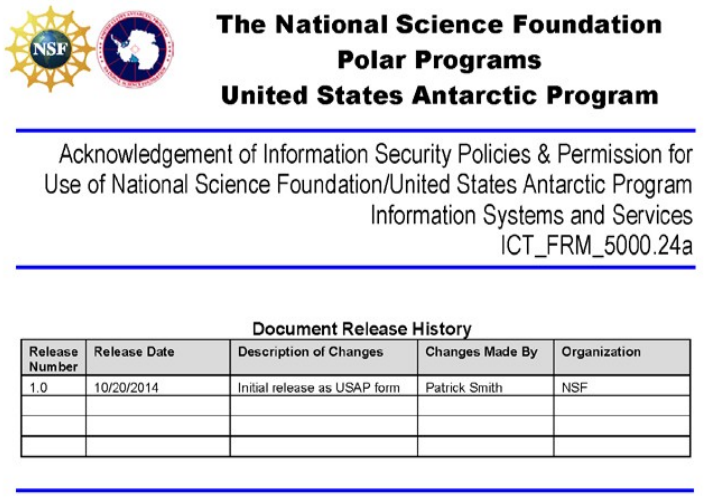
USAP Information Security Policies

Know and abide by NSF/USAP information security policy and guidance and how it affects your use of USAP information technology resources.
USAP security policies are located at:
http://www.usap.gov/technology/contentHandler.cfm?id=1563
Violation of any of these policies can result in **disciplinary action** up to and including dismissal or civil or criminal penalties, including personal financial liability for the cost of improper use.

5000.24	USAP Enterprise e Rules of Behavior
5000.24a	Acknowledgement of Information Security Policies
5000.24b	Sensitive Rules of Behavior and Acknowledgement
5000.01	The USAP Information Security Program
5000.02	Information Security Organization and Administration
5000.03	Information Categorization
5000.04	Risk Management
5000.05	Information Security Architecture
5000.06	Acceptable Use of USAP Information Resources
5000.07	User Access Control Policy
5000.08	Security Auditing Policy
5000.09	Awareness, Training and Education Program
5000.10	Personnel Security Policy
5000.11	Information Resources Physical Security Policy
5000.12	Incident Management
5000.13	Contingency and Disaster Recovery Program
5000.14	Software Management and Protection
5000.15	Information Resource Configuration Management
5000.16	Certification and Accreditation Program
5000.17	Non-USAP Systems
5000.19	Identification and Authentication Policy
5000.20	System Maintenance Policy
5000.21	System and Communications Protection Policy
5000.22	Media Protection Policy
5000.23	System and Services Acquisition Policy

USAP Information Security Policies (2)

All users must sign NSF ICT-FRM-500.24a, *Acknowledgement of Information Security Policies & Permission for Use of NSF/USAP Information Systems & Services.*



The National Science Foundation
Polar Programs
United States Antarctic Program

Acknowledgement of Information Security Policies & Permission for Use of National Science Foundation/United States Antarctic Program Information Systems and Services
ICT_FRM_5000.24a

Document Release History

Release Number	Release Date	Description of Changes	Changes Made By	Organization
1.0	10/20/2014	Initial release as USAP form	Patrick Smith	NSF

By signing this form, you are acknowledging:

- Use of this network requires compliance with USAP policies, rules of behavior, procedures and guidance.
- Mandatory awareness training has been completed
- There is no expectation of privacy and that you consent to being monitored
- Tampering with any information system or network equipment is prohibited
- That you have a responsibility to protect all Government owned information

NSF Information Security Acknowledgement
United States Antarctic Program
October 20, 2014
HARDCOPY UNCONTROLLED – Verify Effective Date Prior to Use
Page 1

Acceptable Uses

Personal telephone and fax usage:
With minimal cost to the government

Personal use of e-mail:
Provided it does not interfere with the participant's work or the work of others and does not incur excessive use of government resources.

Personal use of the Internet:
At the Antarctic stations and vessels, this cannot disrupt mission operations and science support due to excessive bandwidth consumption. Also, all personal use has to comply with Acceptable Use policy (e.g., the full EntROB)

Web cameras and collaborative computing:
Web cameras for training, meetings, educational outreach programs, official business, or personal use is permitted according to USAP policy and with the approval of NSF.

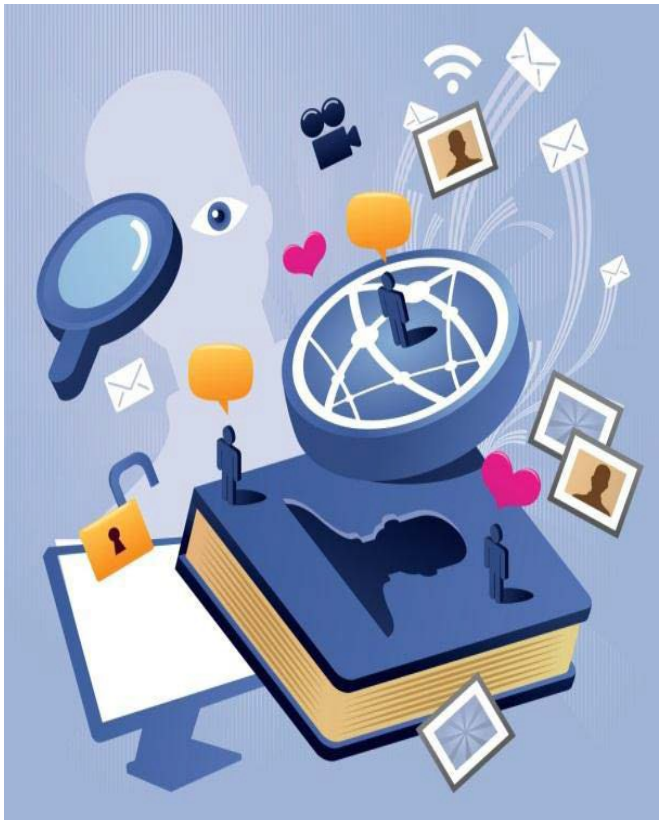
Wireless:
USAP Information Technology services manages wireless access points for connecting to the USAP network. Requests for access must be made through the local Help Desk.

Acceptable Uses (2)

Radio communications:

All official use radio transmission systems require authorization from the USAP Spectrum Manager. See your organizational IT contact person for further guidance.

Personal radio communications devices (e.g. smartphones, walkie talkies, other consumer grade electronics, etc.) must not cause harmful interference to authorized radio communications. Personal radio communications found to disrupt or otherwise harmfully interfere with official communications shall be immediately discontinued permanently.



VPN and Secure Shell Services:

Virtual Private Networks (VPN) & Secure Shell (SSH) are authorized for official business use, only. These services shall be registered and authorized prior to use on the USAP network.

Prohibited Uses

To protect information resources and abide by U.S Law, the following activities are prohibited on the USAP network.

Illegal activities:

All illegal activity is EXPLICITLY forbidden. Examples Include: copyright infringement, gambling, accessing or storing pornography, etc.

Adverse Activities:

Any activity that could adversely affect NSF or US Government interests, interfere with The performance of the USAP mission. Examples include: running a commercial or personal business.

Prohibited Uses (2)

Things you should **NEVER** do while you are using the USAP network:

Examples:

- **Downloading illegal copyrighted materials**
- **Installing unauthorized software**
- **Hacking /cracking systems**
- **Misuse of Email**
- **Create a hostile environment**

  Under no circumstance is it permissible to access or download material that would create a hostile or offensive work environment, such as racist or sexually explicit material.

- **Identity Cloaking**

  Any software or tool used in an attempt to hide the user's identity (e.g. web traffic anonymizers)

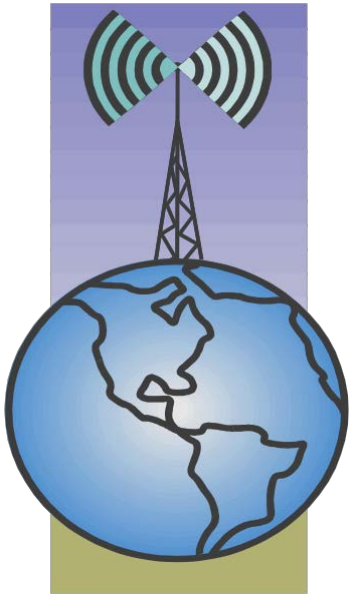
- **Downloading, installing or storing malicious software**
- **Physically altering configuration settings on USAP Equipment** and explicitly attempting to circumvent information security protections.
- Installing or using a non-USAP wireless access point (unless specifically authorized by NSF).

Prohibited Uses (3)

Peer-to-Peer (P2P) Services and Software:

Internet-based peer-to-peer software enables users to access or share files on the workstations of other users across the Internet. Such software allows users to search the network for files that may interest them, and to bring those files to their own computers. Examples of P2P software sites include but are not limited to: KaZaa, LimeWire and BitComet.

***Note: Skype does not fall into this category of P2P. However, Skype use must be approved by the NSF.**



Bandwidth Limitations:

Each Antarctic station and research vessel has limited Internet bandwidth available. To protect that limited bandwidth:

Streaming media services are prohibited

Skype, FaceTime and similar personal applications are prohibited for personal use. These services must be formally requested and approved for business purposes (e.g. grantee educational outreach)

Acceptable personal use may be limited if it negatively affects the USAP mission.

Internet gaming that uses too much bandwidth are prohibited.

Prohibited Uses (4)

Online Representation:

If you can be identified as a USAP participant online, you are responsible for assuring that your postings are not seen as being adverse to the USAP or do not contain hostile material.

Some examples of activities that should not be discussed are:

- The effectiveness of USAP processes and facilities in a public forum.
- How the USAP is spending funding
- Distributing sensitive information about USAP operations
- Representing yourself in a public forum as speaking for the USAP or the NSF.
- Using USAP or NSF logos and titles unless authorized by NSF.

Chat Room and News Group Participation:

Posts to chat rooms and news groups are prohibited activities when such activity results in a display or recording of the participant's identity as affiliated with the USAP.

You are responsible for what you post on the Internet and communicate via Email.

Prohibited Uses (5)

Examples of Misuse of IT Resources

If you are still not sure what constitutes a misuse of NSF IT resources, here are a few more examples:

Downloading illegal copyrighted materials - A summer contractor is caught downloading copyrighted movies from the Internet and burning them to a DVD.

Installing unauthorized software - A staff member installs unauthorized gaming software on their USAP workstation.

Hacking - An employee's child used Dad's USAP laptop, hacked into her high school's academic database, and changed grades for her friends.

Misuse of Email - As the president of his investment club, the management analyst used his NSF email account for sending out correspondence and newsletters to all club members.

Grantee Instrumentation

In the case of approved science activities, all web services, file transfer services, and SSH services required for project support must be listed in the support requirements section of the user's science proposal, Support Information Packet (SIP), Research Support Plan (RSP), and approved by NSF.

Please consult IT Support Staff for guidance.

Sensitive Information

These days it's easy to get overwhelmed with information - it's a constant job to organize, prioritize, and ensure we follow policies to protect information. Although all information has some degree of sensitivity, certain types of information require greater protection.

USAP Participants have a variety of sensitive information available to them electronically and in hard copy. Although the majority of sensitive information maintained by USAP is in systems of records protected under the Privacy Act of 1974 (5 U.S.C. §) such as medical and employment information.
In the course of performing official duties, you may have the need to access this information.

You are responsible for recognizing sensitive information and avoiding inappropriate access, use, or disclosure.

What Is Sensitive Information?

Sensitive Information:

Sensitive information is data that must be protected from unauthorized access to safeguard the **privacy** or **security** of an individual or organization.

Business or Mission Identifiable Information:

Information defined in the Freedom of Information Act (FOIA) as trade secrets or commercial or financial information, that is obtained from a person representing a business entity, and which is privileged and confidential (e.g., Title 13) and exempt from automatic release under FOIA. Also included is commercial or other information that, although it may not be exempt from release under the FOIA, is exempt from disclosure by law (e.g., Title 13).

Sensitive Information (2)

Personally Identifiable Information, or PII, is a subset of sensitive information. It refers to information which can be used to distinguish or trace an individual's identity. It also includes any information that could be used to reference other data elements that are used for identification, such as gender, race, and date of birth.

A name alone is NOT personally identifiable information. A name becomes personally identifiable information only when it is combined with a Social Security Number or with other personal or identifying information, such as:

- Date and place-of-birth,
- Mother's maiden name and Passport number
- Bank account or credit card information, and home address.

Information may also exist in other types of records, such as databases, log files, e-mail and correspondence files. In the course of performing official duties, **you** are responsible for recognizing sensitive information and avoiding inappropriate access, use or disclosure.

Sensitive Information (3)

Sensitive information may come in the form of Business Sensitive Information, Personally Identifiable Information, or Privacy Act Protected Information.

Business/Mission Sensitive Information

Examples:

- System vulnerability reports
- Procurement documentation, including work statements
- Computer security event reports
- Network diagrams
- Commercial proprietary data bound under non-disclosure agreements

Personally Identifiable Information (PII)

Examples (Any combination):

- Driver's license number
- Passport
- Personal email
- Place & Date of birth
- Social Security number
- Credit card information
- Home address, telephone

You are responsible for recognizing and protecting sensitive and personal information contained in USAP files.

USAP Sensitive Information

USAP Sensitive information resides primarily (not exclusively) in the following applications:

- **ACS Firehouse**

  Supports incident reporting and compliance inspections for the Fire Operations Center in McMurdo.

- **Clinical Management Databases (CMD)**
  - Patient tracking Database & Pharmacy Inventory Database
    Tracks patient visits to the USAP medical clinics & prescription drug inventory.

- **MedTech**

  Links health information such as prescriptions, lab results, etc.

- **Pipeline**

  USAP participant deployment information

- **POLAR ICE**

  Scientific Research deployment information

- **Teleradiology**

  Used to transmit medical images and enable video teleconferencing to support medical consultations for patients at Antarctic locations.

- **Travel Accommodations Records Data Information System (TARDIS)**

  Records travel information (e.g., flight, hotel information, and dates) for all personnel deploying through Christchurch.

- **Email**

Protecting Sensitive Information

How Should I Protect Sensitive information:

Restrict access:
To reduce the volume of sensitive information in the USAP, sensitive documents, emails, and files must be **shredded, deleted, or disposed of** in the appropriate manner when no long needed for work purposes.

Store and transmit:
USAP information should only be stored and transmitted on USAP approved devices. For example, encryption must be used to secure sensitive information stored on laptops, portable devices and storage media.

Access to records must be restricted to those who have a **need to know** the information contained in them to perform their official duties.

Records containing sensitive information must be physically secured against unauthorized use and must **NEVER** be left exposed.

Protecting Sensitive Information (2)

How Should I Protect Sensitive information:

- Records containing sensitive information must be physically secured against unauthorized use and must NEVER be left exposed.
- Printer locations must be verified before sensitive documents are sent and documents must be picked up immediately.
- You should always **lock or log off** of your computer when you leave your office.
- Use caution when storing or transporting information in electronic form on portable devices, such as laptops and flash drives.

YOU must protect USAP sensitive information by doing the following:

Confidentiality: Sensitive information should only be accessible to those who are authorized to see it.

Integrity: Only authorized users should be able to make changes to the information.

Availability: Information must be accessible.

Sensitive information is not the same as classified information, which is a type of sensitive information in which access is governed by Presidential Executive Order.

Internet Safety

Spam is unsolicited email sent to many people, and is often used for identity theft or to distribute spyware and malware.

Spyware monitors your computer, observes your Internet habits, and can report back what it sees. It can lead to identity theft and theft of other personal information.

- **Ignore** unsolicited email and unwanted advertisements
- **NEVER** give personal information
- Do **NOT** click links to web pages
- **NEVER** reply to spam

Internet Safety (2)

Phishing is a method hackers use to gain information from systems. Scammers copy major websites, and send a fake email with a link to the fake site.

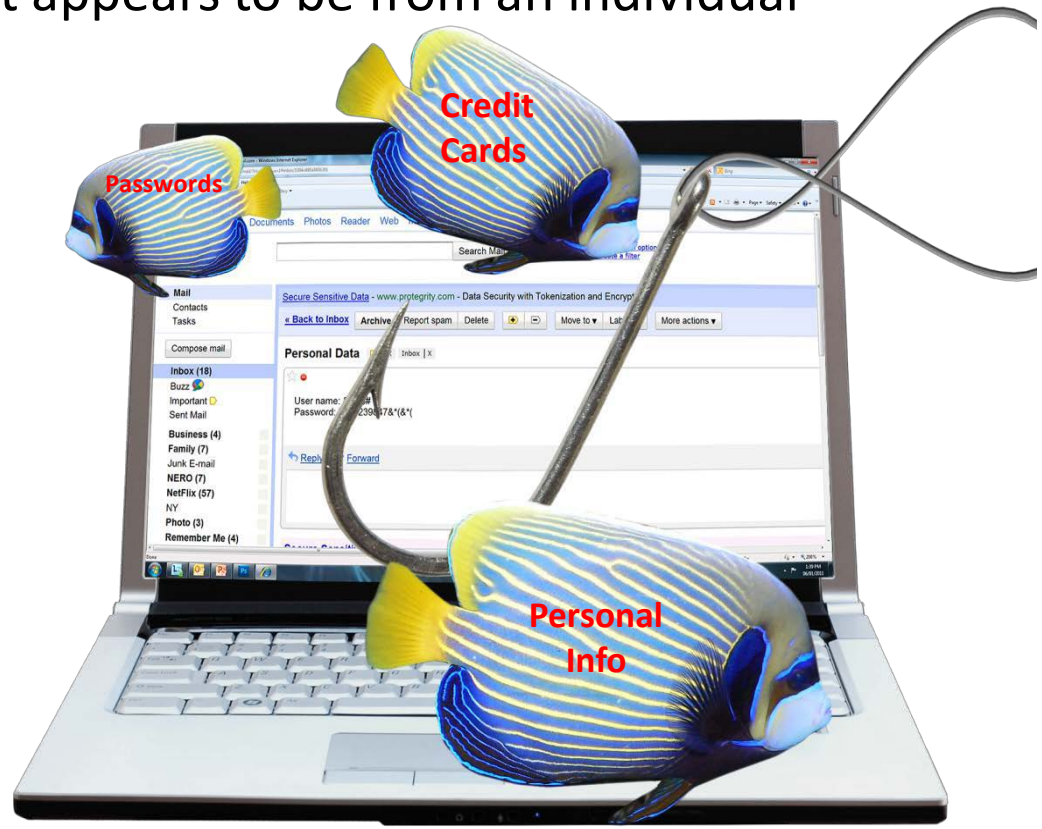
Some of the ways you can tell if you are being "phished":

- An email may include bad grammar, misspellings, and/or generic greetings
- Asks you to update or validate information or click on a link
- Threatens dire consequences or promises rewards
- Appears to direct you to a web site that looks real

Phishing – Resist the Urge to Click!

Internet Safety (3)

Spear phishing is an email that appears to be from an individual or business that you know, but it isn't. It's from the same criminal hackers who want Your credit card and bank account numbers, passwords, and the financial information on your PC.



"The spear phisher thrives on familiarity. He knows your name, your email address, and at least a little about you." -Norton

Don't get caught by the Spear Phishing Hook

Internet Safety (4)

Steps to take to prevent a Phishing Attack:

- **Do not** click on links or attachments in e-mails that you cannot verify.
- **Don't** disclose any personal information in plain text by e-mail.
- **Never** give anyone (not even the Help Desk) your password
- **Contact the sender** of an e-mail to verify a request sent via e-mail
- **Report** suspicious e-mails to your local Help Desk

Preventing A Phishing Attack

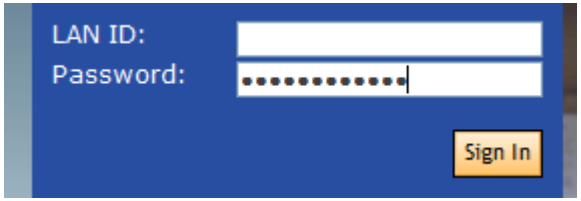
Insider Threat

Not all malicious activity originates from outside of USAP. An Insider threat is a real threat, and is more likely than an external exploit. Insider threats are caused by current or former USAP participant(s) who has or had access to USAP information or information systems; and purposely sets out to compromise the confidentiality, integrity or availability of the information or information system.

You have a responsibility to report anything that may be suspicious, inappropriate or that may result in increased risk to the USAP mission!

Passwords

Using passwords is one of the most basic methods of improving information security. This measure reduces the number of people who have easy access to the information, since only those with approved codes can reach it. Unfortunately, passwords are not foolproof, and hacking programs can run through millions of possible codes in just seconds. Passwords can also be breached through carelessness, such as by leaving a public computer logged into an account or using a too simple code, like "password" or "1234."



To make access as secure as possible, users should create passwords that use a mix of upper and lowercase letters, numbers, and symbols, and avoid easily guessed combinations such as birthdays or family names. People should not write down passwords on papers left near the computer, and should use different passwords for each account. For better security, a computer user may want to consider switching to a new password every few months.

Weak and Default Passwords

Weak and default passwords are easily guessed. They include:

- Words found in the dictionary
- Information significant to you (names, dates, cities, etc.)

This may allow a hacker to:

- Attempt to use your password across multiple sites and systems
- Crack passwords to less secure sites
- Access your personal or USAP official information

Password Requirements

NEVER SHARE YOUR PASSWORD WITH OTHERS AND PROTECT FROM INADVERTENT DISCLOSURE.

Your password must be a minimum of **12 alphanumeric characters**.

- Does **not contain three or more** consecutive characters from your username.
- Contains a **combination of characters** from at least three of the following categories:
  - ✓ English uppercase characters (**A-Z**)
  - ✓ English lowercase characters (**a-z**)
  - ✓ Base 10 digits (**0-9**)
  - ✓ Non-alphanumeric characters (for example: **!**, **$**, **#**, or **%**)

Examples of Strong Passwords:
D@rkg066Le$$ (Dark goggles)
Tr@vel2Ant@rctica (Travel to Antarctica)

Your password expires every 60 days and cannot be reused for one year.

How to Encrypt Files

Microsoft Office

1. Open the file you want to encrypt
2. Click “File” located to the far left above the Ribbon
3. Choose “Info”
4. Click the downward pointing arrow below “Protect Document, workbook in excel or presentation in PowerPoint” from the resulting “Info” menu.
5. Choose “Encrypt with Password” from the resulting document protection menu.
6. Using a strong password, enter your desired password into the resulting dialog window then click “OK” to finish encrypting the file.
7. If emailing the file, send the password in a separate email.

Adobe Acrobat Professional

1. Open the file you want to encrypt
2. Click “File” located to the far left above the Ribbon
3. Choose “Properties”
4. Click the “Security Tab”
5. Under Security Method choose “password security”
6. Click the check box “Require a password to open the document”
7. Using a strong password, enter your desired password into the resulting dialog window then click “OK” to finish encrypting the file.
8. If emailing the file, send the password in a separate email.

Removable Media

Removable storage devices are vulnerable to loss or theft.

- Examples:
  - CD /DVD
  - external hard drives
  - flash drives, thumb drives
  - cell phones and smart phones; such as PDAs, Blackberry, or iPhones.

- FIPS 140-2 compliant encryption must be used on all removable storage devices containing NSF/USAP data. Please contact the Help Desk for assistance.

Removable Media Protection:

Do not plug a thumb (flash) drive into your computer if you do not know the owner

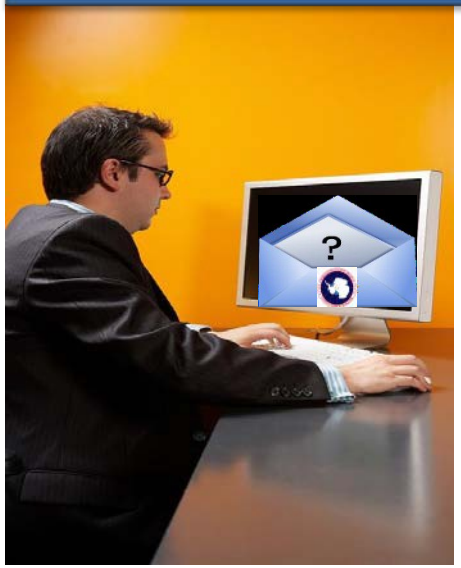
Do not plug a thumb drive or load a CD/DVD into your computer if it was a "giveaway" as a prize or free product trial.

Ensure that the "autorun" setting on Windows computers is disabled

Scan any removable drives. If you don't you may expose your computer becoming

corrupted or allowing a hacker to have access to your system.

Email Etiquette



In order to use email safely and correctly, you might want to ask yourself these simple questions before you hit the send button.

Should this message be from NSF/USAP?
When you send or forward messages from the USAP, they identify the agency. This action lends your name and the NSF reputation to the message. NSF email is the same as using NSF/USAP letterhead.

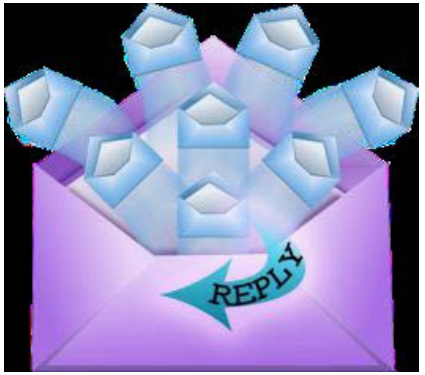
Should I send this via email? Certain information should not be sent by email, such as personal information.

Is the language and content appropriate?
Email is neither confidential nor private and you should assume that anyone may see your message. You might want to reconsider your words. There should be no sexually explicit, racist, or other offensive language in the message.

Email Etiquette (2)

- **Do NOT** send Social Security Numbers through email. USAP email is **NOT** encrypted when emails are sent within the email system. Email forwarded outside the NSF email system is **NOT** encrypted. For example, email forwarded to Gmail or another agency system is **NOT** encrypted in transit.

A little email etiquette goes a long way.



- **Think** before acting, but be prompt in your reply.
- Be clear and organized and use meaningful text in the subject line.
- Only copy people who need to be informed.
- **Be professional** at all times and avoid inappropriate language.

Your USAP email may be considered a **federal record** and may be subject to request under the Freedom of Information Act (FOIA). Any email message in your USAP account may be reviewed by NSF management, the Inspector General's office, or law enforcement.

- **Remember:** Don't respond to an entire group list if you only need to respond to one individual. Always respect people's time.

What Can I Do?

Know your responsibilities:

- Acceptable Uses
- Prohibited Uses
- PII & Sensitive data when you see it and how to protect it.

Be Aware of :

- SPAM
- Malware/Spyware
- Phishing VS. Spear Phishing
- Social Engineering
- Insider Threats

Implement Secure Practices:

- Strong Passwords
- Restrict disclosure of information
- Always lock or log off computer
- Alert supervisor or call Help Desk if you see suspicious activity.

If you are not sure **Contact** your Supervisor or the local Help Desk!!

Reporting an Incident

In the event of a suspected or confirmed breach of these information security policies and procedures you must **immediately** report the event to your local Help Desk.

If you realize you've been a victim of a phishing attack or if there is suspicious activity on your computer, report it to your local Help Desk.

Contact Information

If you have any questions, or need to report suspicious activity or an incident, use the contact information below based on your location.

For USAP operating locations in the US (Denver, CO; Charleston, SC; Port Hueneme, CA; or offices in Arlington, VA and Galveston, TX), please contact:

USAP Enterprise Help Desk

helpdesk@usap.gov / 720-568-2001

For the Christchurch, NZ USAP operating location, please contact:

Christchurch Help Desk

chc-helpdesk@usap.gov / x35420

For the Punta Arenas, Chile USAP operating location, please contact:

USAP Enterprise Help Desk

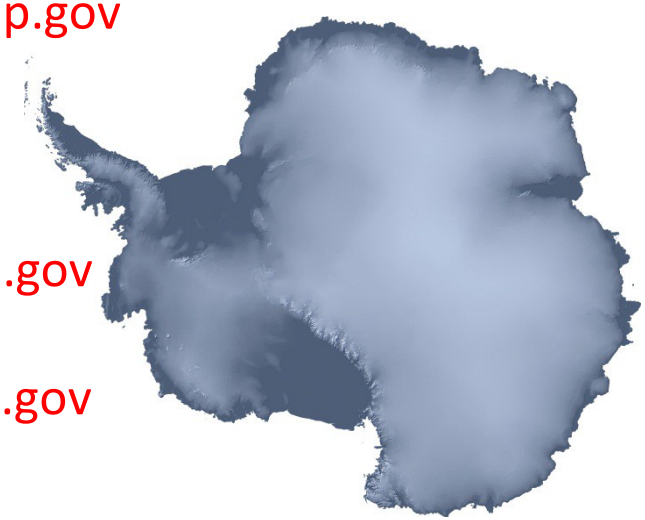
helpdesk@usap.gov / 720-568-2001

Contact Information

For Antarctic stations and vessels, please contact:

Palmer Station:
Palmer.helpdesk@usap.gov
x52794

Research Vessels:
LMG: admin@lmg.usap.gov
x52855
NBP: admin@nbp.usap.gov
x52861



South Pole Station: POL-helpdesk@usap.gov
x61603 (winter)
x61801 (summer)

McMurdo Station:
MCM-helpdesk@usap.gov
x3700

Summary

- The protection of the USAP network and the information that resides on it depends on **you**.
- Failing to do your part increases risks to the network and could lead to a compromise for which **you** could be held responsible.
- Use of NSF USAP information systems is a **privilege**.
- Failure to comply with required information security requirements could result in a temporary or permanent loss of your network usage.