United States Antarctic Program
INFORMATION SECURITY AWARENESS

Information Security Awareness Training is a Federal Requirement

This course explains why information security is important, and describes acceptable and prohibited uses of USAP resources. By completing this course you meet the requirement that applies to all USAP participants for completing federal information security awareness training prior to receiving access to the USAP network.

Why Information Security is Important

Information security is a responsibility of and affects all USAP participants who use the USAP network to

- access the Internet;
- transport science data to a home institution;
- perform a job;
- check email.

By acknowledging the USAP Enterprise Rules of Behavior (EntROB) later in this course, and by accepting a USAP network account, you acknowledge your accountability to comply with the guidelines described in this course for using USAP infrastructure or equipment.

What is your role in Information Security?

As a USAP participant you play a critical role in information security. During your day-to-day operations, you can best protect USAP resources by doing the following:

- **Be Proactive**
  Adopt good security best practices as described in this course.
- **Be a Learner**
  Understand security threats that affect the USAP environment.
- **Seek Help and Advice**
  Contact USAP Information Security personnel with questions to find out more 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 the IT Help Desk at your location or IT personnel.

Location of USAP Information Security Policies

All USAP participants are required to know where to find the Information Security policies. The policies are listed on the USAP Information Security Program web pages (under Technology on www.usap.gov).

Expectation of Privacy

The USAP logon banner depicted here is presented every time you log on to the USAP network. It is a reminder that you cannot expect privacy when on the USAP network.

USAP-provided equipment that transmits or receives data, such as email, smart phones, and mobile devices, are the property of the NSF and are subject to monitoring.

If you prefer not to have your personal communications subject to the monitoring, use a web-based mail service, and do not store personal messages or files on USAP network or desktop storage systems, or USAP-provided devices.

The NSF does not possess the requisite infrastructure and resources necessary to guarantee the privacy of information processed or stored on USAP resources. Users of USAP systems accept 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.

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. In doing so, the administrators do not release any information to the public or unauthorized persons.

Acceptable Uses of USAP Resources

USAP information resources are provided for operational, science, and recreational use. When using USAP resources, you are expected to go beyond following the guidelines provided in the USAP Enterprise Rules of Behavior by using your best judgment and highest ethical standards to guide your actions.

If an acceptable use activity is found to negatively impact the USAP, such as creating bandwidth congestion or transmitting or downloading prohibited material, the activity may be temporarily limited or banned.

The basic guideline when using USAP resources is to avoid prohibited uses or activities that may negatively impact or interfere with the USAP mission.

NOTE: See the Prohibited Activities section for an explanation of what is not allowed.

Examples of **acceptable uses of USAP resources** include the following:

- Personal email
- Internet browsing
- Instant messaging
- Election material
- Encryption of personal transmissions
- Third-party software
- Internal network gaming

Personal Email, Internet Browsing, Instant Messaging

General use of the Internet for personal communications is acceptable as long as these activities do not create bandwidth congestion or are used to transmit or download prohibited material.

Election Material

- You can distribute information on how to participate in U.S. federal, state and local elections.
- You cannot advocate for or against an issue or candidate while representing the USAP, RPSC, or the NSF.
- You are not permitted to register with a political organization as affiliated with the USAP, RPSC, or the NSF, or by using your USAP email address.

Encryption of Personal Transmissions

You may encrypt personal emails or data files stored on a personally owned system; however, encrypted communications are subject to monitoring and authorized auditing. In the case of an authorized investigation you may be required to provide officials with the passphrase used to encrypt the data file or communication.

Third-party Software on USAP Systems

With prior management approval, USAP personnel may install software on a government system when the software is required to support their work responsibilities. For information on receiving approval to install software on a USAP system, email the Denver IT Help Desk (HelpDesk@usap.gov).

Internal Network Gaming

Network gaming internal to the local network that does not impact bandwidth (i.e., is not done over the Internet) may be allowed with management approval.

Prohibited Activities

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

NOTE: The network communications, infrastructure and information systems are monitored for violations, and authorities are notified when necessary.

- Illegal or harmful activities
- Misuse of representation of your USAP identity online
- Distribution of materials interpreted as adverse or hostile
- Transmission of classified information
- Sharing account access information

- Enrolling others in list services
- Setting up personal information services
- Internet network gaming
- Violation of copyright law
- Use of peer-to-peer applications
- Excessive bandwidth use
- Violations of the Enterprise Rules of Behavior (EntROB)

Guidelines on prohibited uses are provided below and later in this course.

Illegal Activities
Upon detection law enforcement authorities are notified.

Harmful Activities
Activities that may harm USAP systems or the network infrastructure are prohibited.

Classified Information
Storing, processing, or transmitting government classified information is prohibited on the USAP network.

Enrolling Others in List Services
You are not authorized to enroll other USAP participants in mailing lists, chat room lists, or other list services without their consent.

Personal Information Services
The following are prohibited:

- Using personal servers for email, web, ftp, telnet, etc., or wireless access points, wireless routers, switches/hubs and other network infrastructure.
- Hosting a chat room or newsgroup for personal, e-commerce, or non-program business activities.
- Using tools to monitor network traffic activity or content unless authorized by the NSF and required for your job.
- Using servers and network equipment connecting to the USAP network that were not identified in a Research Support Plan and/or do not have NSF approval (for example, additional science equipment).

Network Gaming Activities over the Internet
Network gaming over the Internet is prohibited due to the impact on USAP bandwidth resources.

Content Filtering

The following are prohibited material on the USAP network:

- Web sites with the following:
  - Sexually explicit material
  - Forms of gambling
  - Hate rhetoric
- Anonymizers (tools that allow a user to anonymously use the Internet)
- Peer-2-Peer File Sharing (tools that use peer-to-peer protocols such as Skype)

If you attempt to access a restricted web site, your browser may display the following message:

Notice

NSF has blocked access to this site.

If you believe you have received this message erroneously, with respect to an appropriate site, please submit a request to the USAP Help Desk at HelpDesk@usap.gov.

If the web site you are attempting to access is necessary for you to perform your research or to complete your job function in support of the USAP mission, send the web site address (URL) to HelpDesk@usap.gov for evaluation.

Remember: When using USAP resources for work related activities and personal use, go beyond the stated rules of the EntROB and use your best judgment and highest ethical standards to guide your actions.

Why Peer-to-Peer Applications Are Prohibited

Peer-to-peer (P2P) applications exchange data between computers without the use of a centralized server, which allows users to interact directly with each other to share information.

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

- Skype™

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

More on Skype

Skype uses a proprietary Internet telephony (VoIP) network. The main difference between Skype and standard VoIP clients is that Skype operates on a peer-to-peer model (originally based on the KaZaA software). Additionally, Skype does not meet federal information security requirements and therefore is not allowed on the USAP network.

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

Dangers and Risks of P2P	• Not protected by USAP security systems.
	• Consumes significant bandwidth resources.
	• Can lead to the following:
	  o Spreading of Viruses, SpyWare, Trojan horses.
	  o Compromise of your privacy.

Items That Are Not P2P	• Instant messaging (e.g., MSN Messenger®, AOL Instant Messenger™) • Group meeting software (e.g., WebEx™, Centra®, Microsoft® NetMeeting®)
What To Do if P2P Applications Are Already Installed on Your Computer	Contact the IT Help Desk. The IT Help Desk informs USAP IT technicians who assist with removing P2P applications. (P2P applications are difficult to remove, as they modify registry values and have many associated adware programs.)

Copyright Infringement

WARNING

Violation of copyright laws is considered an illegal activity, and is not tolerated on the USAP network. USAP network and share drives are periodically monitored for violations.

Federal law prohibits unauthorized copying, sharing, or distribution of copyrighted materials. Examples of copyrighted material include the following:

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

This **does not apply** to the legal purchase of music or video entertainment within bandwidth restrictions.

Representation of USAP Identity Online

If you can be identified as a USAP participant while online, you are responsible for assuring that your postings to public web sites, blogs, and chat rooms cannot be interpreted as **adverse activity** or **hostile material**. Additionally, the general public may improperly view USAP participants as representatives of the USAP or the NSF. USAP participants are not allowed to represent themselves as U.S. government officials.

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

If you post information or commentary that is viewed as negatively impacting the USAP mission or the interests of the NSF, you may be subject to administrative, civil, or criminal penalties.

Adverse Activity

As a USAP participant, you agree that you will not create or distribute material that may be interpreted as negatively impacting the interests of the NSF or interfering or negatively impacting the USAP mission.

Examples of what may be interpreted as adverse activities:

- Discussing the effectiveness of USAP processes and facilities in a public forum.
- Discussing how the USAP is spending funding in a public forum.
- Distributing sensitive information about USAP operations to individuals who are not authorized to receive that information.
- Representing yourself in a public forum as speaking for the USAP or the NSF.
- Using USAP or NSF logos and titles unless specifically authorized by the NSF.

Adverse Activity Scenario

James has been working as a carpenter in the USAP for five years and is frustrated that the carpenter shop in McMurdo is not receiving increased funding next year to replace equipment. James posts his opinion that the NSF is not properly funding the USAP program on his MySpace page, which is publicly accessible to anyone on the Internet.

Dr. Smith who is interested in pursuing a grant with the USAP for scientific research at McMurdo station reads James' MySpace page and is concerned about the lack of funding for the carpenter shop. Dr. Smith emails the NSF representative he is working with to ask about the situation.

The NSF representative researches the problem and finds out that the carpenter shop has been inspected and is not due for replacement equipment for two more years. The NSF representative informs Dr. Smith that the information he read on MySpace was posted by someone who was misinformed of the situation at McMurdo.

How should James have addressed his concerns instead of posting information to the Internet that was interpreted as an adverse activity to the USAP mission?

Resolution

The best way for James to address his concerns is to ask his supervisor for information on the status of replacement equipment instead of posting his concerns on a public forum. If James knew that funding was planned for the carpenter shop in two years, he may have reconsidered posting complaints online.

Hostile Material

As a USAP participant, you agree that you will not create, distribute, transmit, store, or intentionally view pornographic, sexist, racist or threatening material on the USAP network or a USAP system, in a USAP work space, or in a publicly accessible area.

Examples of actions that may be interpreted as hostile material:

- Updating a public web site with stories of events that occurred on station that may be interpreted as defamatory, slanderous, or insulting to people involved in the event.
- Sending an email, instant message, or voicemail to other USAP participants containing personal opinions that are insulting to a political party or public figure.
- Using verbal, written, or electronically generated hate speech.
- Posting slanderous material about other USAP participants, USAP personnel, or NSF representatives to a public web site, or via email to other USAP participants.

Cyber-Bullying

Cyber-bullying is any online communication that may be interpreted as hostile by the recipient or the individual who is the subject of the communication.

Examples:

- Repeatedly sending emails to a person who has said he/she wants no further contact with you.
- Making threats, sexual remarks, or using hate speech in text messages.
- Ganging up on a person by making him/her the subject of ridicule in a group email or public forum.
- Posting statements or gossip to humiliate someone.
- Disclosing someone's personal data (real name, address, or workplace/schools) on a web site or forum without the person's consent.

Hostile Material Scenario

A project is running into logistical challenges with getting materials to Palmer Station in time for a research project to start. Tom, the Logistics Manager, emails the team stating that Sandy, another team member, is the reason for the delay and should be fired. Others on the team lose confidence that the logistics problem will be addressed due to internal fighting.

How should Tom have addressed his concern instead of sending an email that was interpreted as hostile material?

Resolution

Tom should have spoken with his supervisor rather than send an email to a group of USAP participants that was interpreted as slanderous. Sandy has the right to escalate the email to USAP management and NSF authorities. If the NSF deemed appropriate in this case, Tom would be subject to penalties for creating a hostile environment.

USAP IT Best Practices

All USAP participants are expected to adhere to the following best practices:

- Password Protection
- System Maintenance
- Physical Security
- Web and Email Use

Password Protection

The USAP network account issued to you is only to be used by you to access the network.

It is prohibited to allow someone else to use your login information or your USAP email account. You must protect your USAP password; it serves as an important "first layer" in protection for the USAP network, and it protects you from someone using your access to perform prohibited or destructive activities.

The USAP network is a federal government network, therefore, when you create a password, it must meet the following requirements:

- Must be a minimum of **twelve 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 **%**)
- **Expires every 60 days** and is not reused for one year.

Password/Passphrase Tips

- Change your password regularly.
- Make the password easy to remember and hard to guess.
- Protect your password. **Do not** share passwords or write them down.

Examples of Strong Passwords

- **D@rkg066Le$$** (Dark goggles)
- **Tr@vel2Ant@rctica** (Travel to Antarctica)

Personal Systems

When using a personally owned system on the USAP network, be sure the operating system provides password protection capabilities.

Examples:

- MS Windows® XP and Apple Macintosh® provide password protection.
- MS Windows 95/98/ME **do not** provide password protection.

System Maintenance

All systems connected to the USAP network are subject to continuous monitoring. Network traffic monitoring and vulnerability scans are used to do the following:

- Monitor quality of service.
- Detect violations of the USAP EntROB.
- Identify potential weaknesses in the system that may pose a risk to the USAP network (vulnerabilities, attacks, threats).

If a weakness is detected on your system, Information Security notifies you via email or in person. Upon notification, you are required to address identified weaknesses in a timely manner or the system's access to the network may be revoked. If your system is deemed by the NSF as an unacceptable threat to the network, your system may be disconnected without notice.

Maintaining Your System

Ways to properly maintain your system to lower the likelihood of being identified as a risk to the network include the following:

- Maintaining current patches for the operating system and software applications installed on your system.
- Updating antivirus definitions daily.
- Running the current version of your antivirus software.
- Remediating vulnerabilities in a timely manner.

Antivirus Protection

All computers connected to the USAP network are required to run active and current antivirus software. When using a personal system on the USAP network you are required to assure that antivirus definition files are kept up-to-date, which can be achieved by enabling the auto-update option.

Physical Security

Physical security includes being cautious of theft of and remote access to your portable devices.

Theft of Mobile Devices

Laptop and mobile phone theft is a recurring threat, especially while traveling. Always maintain visual or physical contact with your laptop, smart phone, or mobile device, and never check in a laptop or mobile device as luggage. Be especially vigilant of your equipment while in airports and traveling on buses, trains, shuttles, and taxis.

Immediately report loss or theft of personal or U.S. government computer equipment to an IT manager or the IT Help Desk at your location.

Potential for Remote Access to Your Device

When using a portable device in a public networking environment, such as using wireless at an airport, be sure your device is not configured to allow for unauthenticated access or file sharing. This is especially important when using WiFi, BlueTooth, or infrared applications.

- If your device is configured for unauthenticated access, anyone can connect to your machine.
- If your device is configured for unauthenticated access and file sharing, anyone can access all the files on your machine.

Shoulder Surfing

Shoulder surfing is when someone observes a person using a computer with the intent of obtaining information. For example, watching someone enter a PIN at an ATM or a username and password on a web site.

As a USAP participant, it is important to be aware of your surroundings when accessing sensitive information at the office, and when using a computer in a public environment, such as an airport or on an airplane.

Methods of Preventing Shoulder Surfing

In the office:

- When away from your desk or cubicle, lock your workstation (**Windows Key + L** or **Ctrl + Alt + Del** and then **Enter**).
- If your back is to the entrance of your work space, hang a mirror in your line of sight in order to see when someone is standing behind you.

Do not view sensitive information when someone who may not have authority to view the information is in your workspace.

In a public environment:

- Be aware of your surroundings, especially if there are people behind you who can view the screen you are working on, such as on an airplane or at a computer kiosk.
- Avoid entering usernames and passwords or viewing sensitive information when in a crowded environment.
- Shield paperwork from observation.
- Shield keyboards from view (so someone cannot see you enter a pin or password).

Use a privacy filter on your laptop to limit the range of view to your screen.

NOTE: If you use a privacy filter, someone directly behind you such as on an airplane can still view the screen.

Web and Email Use

When using the Web or email, be aware of the following:

- Threats to information resources

- Deceptive practices on the Internet
- Fraudulent emails
- Fraud in Instant Messaging (IM)

Threats to Information Resources

Information security practices are designed to protect USAP resources, such as bandwidth, medical records, science data, and personal information. Threats to these resources include internal and external:

Internal Threats

- Accidental/intentional loss or change of data
- Fraud, waste, and abuse
- Disgruntled users
- Unethical behavior

External Threats

- Natural disasters (flood, storm damage, fire)
- Criminal events (robbery, arson)
- Information-focused attacks (hackers)

External Threats

External threats most commonly occur in cases of attempted identity theft, phishing, or social engineering.

"You are a winner!"
"Dear Valued Customer,"
"In order to verify your account ..."
"Greetings Sir/Madam, from your beneficiary ..."
"Believe me, this is not a scam!"

Identity Theft
Theft of personally identifiable information (PII) that may be used to compromise personal financial resources (bank accounts, credit cards, stock brokerage accounts).

> **Example:**
> Spyware loaded on a computer that captures social security number (SSN) or bank account number transaction information.

Phishing
The act of falsely claiming in an email to be a legitimate company (such as a bank) in an attempt to deceive someone into surrendering PII to use for identity theft.

> **Example:**
> Email imitating the appearance of an official email from a bank and asking the recipient to verify account information by clicking on the URL provided in the email.

Social Engineering
The acquisition of sensitive information (SI) or inappropriate access privileges, based upon the building of a trusted relationship.

> **Example:**
> Receiving a phone call from someone falsely representing themselves as from the local IT department and asking for you to provide your password in order to conduct a test.

Deceptive Practices on the Internet

As more people use the Internet and become knowledgeable of deceptive practices, forms of technical deception become more complex. To reduce risk to the USAP network, it is important that you are aware of and pay attention to ways you may be prone to deceptive practices.

Look out for the following when using the Internet:

- **Forged Web Sites**
  A fake web site designed to convince you that you are visiting the web site of a trusted organization.
- **Misspelled URLs**
  Designed to make a link in an email and the forged web site it leads to appear to belong to a legitimate organization.
- **Images as Links**
  Use of images instead of text to direct users to a forged web site.
- **Phone Calls**
  A real caller or a recorded message that prompts an individual to enter an account number and PIN to verify their account may be a phishing attempt. Also, caller ID information can be falsified, so this is not always a safe method for verifying that the caller is actually from a trusted organization.

How to Avoid Deceptive Practices

- When contacted to verify sensitive information for a company or affiliation you do business with, **contact the company directly** through means you normally use rather than providing any information directly to the inquirer. For example, go to the web site you normally use for online business rather than clicking on a link provided in an email or Instant Messaging (IM).
- **Be critical** of emails you receive from trusted companies. Typically emails from companies with which you have an account direct the email to you personally by specifying your username or a partial account number in the email. If you receive an email that is directed to a general audience, such as "Dear customer," the email may be a phishing attempt.

Fraudulent Emails

Malicious Internet users are more frequently using fraudulent email for phishing and hacking attempts. Fraudulent emails are also becoming more difficult to detect as senders realize that the more targeted and personal the email, the more genuine it appears to be. For example:

- **Internet Holiday Greeting Card Emails**
  Emails masquerading as greeting cards from your friends or coworkers, when they are actually social engineering attempts to acquire sensitive from you.
- **Malicious Email**
  A company was recently the target of a malicious email campaign. The email, which originated from a Yahoo address, purported to be from a senior corporate official and contained a link to a zip file presented as a screensaver commemorating the company's 85th Anniversary. Upon investigation, the attached file was identified as a malicious program.

Precautions You Can Take

Scrutinize Communications	Scrutinize unexpected emails containing links. If unsure, manually enter the link into your web browser rather than

	clicking on it in the email.
Avoid Disclosing Your Email Address Publicly	Be careful where you post your email address on the Internet. Automated systems scour the Internet for email addresses to add to their spam and MALWARE databases.
Confirm Attachments Before Opening	Before opening an attachment provided in an unexpected email, verbally confirm with the sender that the email and attachment was sent to you, and that the attachment is safe to open.
Report Potential Threats	If you receive an email and suspect it may be an attempt at identify theft or some other malicious activity, contact the Help Desk at your location.

Instant Messaging

Instant Messaging (IM) poses security threats that are in some ways more severe than email because IM provides local access to your system. This means that potential threats, such as viruses, worms or Trojans can directly impact your system if you click on an attachment or URL that activates the threat. Also, MALWARE spread via IM uses your list of IM contacts to infect other systems.

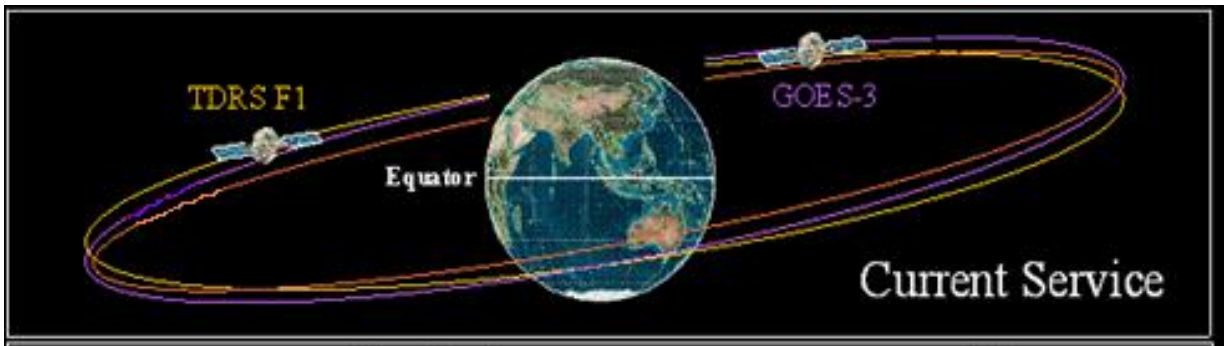
Do the following to avoid IM malicious activities:

- Be wary of links and downloads.
- Protect personal information.
- Be careful on public computers.
- Never respond to unsolicited messages.
- Use encryption.

Bandwidth Information

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. Some uses of bandwidth include support for direct-dial telephone service to the U.S., mission critical operations applications, and support for emergency telemedicine.

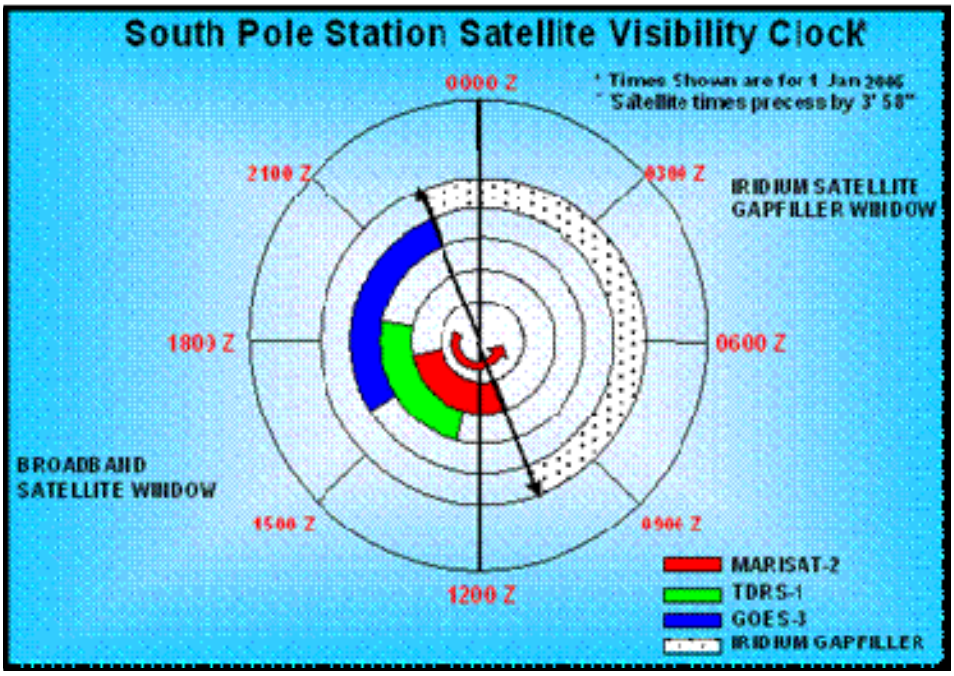
When you're on the USAP network, any personal use of the Internet is secondary to support of basic operations of the program, and to the generation and support of scientific data.



Satellite	Owner	Launch	Year Visible @ Pole	Year In-Service @ Pole	End of Life	Inclination	Transponder Bandwidth	Data Rate	Daily Contact (Hours)	Teleport
GOES-3	NSF	1978	1993	1995	?	13.97 °	8 MHz	1 Mb/s	6.8	Miami, FL
TDRS F1	NASA	1983	1997	1997	~2008	12.56 °	225 MHz	5 Mb/s	6.1	White Sands, NM
"	"	"	"	"	"	"	20/10 MHz	T1	"	"
TDRS F3	NASA	1988	2005	~2009	~2014	9.89 °	225 MHz	150 Mb/s	5.0	White Sands, NM
"	"	"	"	"	"	"	20/10 MHz	T1	"	"
IRIDIUM*	IRIDIUM	1997+	1997	2005	2014	86 °		9.6 Kb/s	24	Wahiawa, HI

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 austral summer season at McMurdo when over 1,000 people are sharing this resource, it is essential that available bandwidth is primarily dedicated to operational and science support requirements.



Bandwidth is limited at South Pole Station based on when satellites are visible to the station. The Internet is not available at South Pole when satellites are not visible to the station.

Bandwidth Usage

When it comes to using bandwidth, there are certain restrictions and limitations.

Potential for Restrictions on Acceptable Uses of USAP Resources

As stated earlier in this course, there are acceptable recreational uses of USAP resources. However, acceptable activities may 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 are notified. Upon further abuse, your supervisor is notified, and your use of the network may be restricted or prohibited.

Please use the USAP network and information systems wisely and courteously. If you have a question about what may or may not impact the USAP mission, contact the Denver IT Help Desk.

Limitations on Authorized Official Use

For those of you who are using the network for authorized official use, such as transferring science data to a 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, update your Support Information Package (SIP) and obtain NSF approval before changing your network use practices. If your network activities exceed your authorized level of service, the NSF may restrict or disconnect your systems.

Media Download over Internet Scenario

While Bob is in McMurdo, his family sends him a $50 iTunes® gift certificate. Bob uses the computer kiosks in Building 155 for personal email, to pay bills, and manage online banking. On his lunch break while at a kiosk Bob notices that ten other people are downloading music and other media files from Internet media downloading services such as iTunes, and complaining about how long it takes to download a file. What should Bob do?

Resolution

While iTunes and other music or video download services are considered acceptable use of the Internet on the USAP network, recreational use must not impact the USAP mission.

In this scenario Bob is witnessing a reduction in the quality of service due to numerous people simultaneously using McMurdo bandwidth for recreational purposes in the middle of the work day. Bob should come back to the kiosk during off-duty hours when less people are downloading files.

If too many people are using the Internet on station for recreational downloads, bandwidth resources become over extended, and USAP mission and science activities are compromised. For example:

- Scientists cannot transmit research data to their home institution.
- Medical cannot transmit x-ray images to New Zealand in the case of a medical evacuation.

- Human Resources cannot transmit payroll information, which delays distribution of payroll for all of the support staff on station.

Streaming Media Scenario

Larry went to his workstation after hours to finish some work, and found Mike at his workstation laughing.

"What's so funny?" Larry asked.

"Oh, it's this show. It's so hilarious I'm addicted to it - I watch it every week."

"How are you watching a T.V. show that's not on the station television channel?"

"Oh, ABC has it on their web site the day after it airs, so we can see it on the Internet."

"I should try that with my favorite shows! Thanks!"

What is the issue with Larry watching his favorite shows via streaming media on the Internet?

Resolution

While several networks offer shows online after the initial broadcast, watching streaming media from any computer on station significantly strains bandwidth. Streaming media requires a constant download of data the entire time you're watching, which affects bandwidth, even during off-hours. Once one person uses streaming media, many people may use it, which will cripple the ability to move any data on the USAP network.

Personally Identifiable Information

Personally Identifiable Information (PII) as defined in OMB-03-22 is information about an individual maintained by an agency that 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 Protecting PII is Important	Doing so • protects USAP participants from potential identity theft; • assures the USAP complies with U.S. federal regulations. As stated in *USAP Information Security Instruction 5000.7-1, Privacy and Sensitive Information Protection*: **All USAP participants are responsible for recognizing sensitive information and avoiding inappropriate access, use, or disclosure.**

Avoiding Disclosure of PII

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.
- Only transmit PII via email if the data is encrypted.
- For storage, transfer, or transport purposes, do not store sensitive information on portable devices such as laptops, smart phones, USB drives, or on remote/home systems unless you have written authorization from you manager 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 a USAP network, system, application, data, paperwork, or other resource that result in the unauthorized release (*spill*) of personally identifiable information (PII).

Examples:

- 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

Summary

Key points addressed by this course to keep in mind when using USAP resources:

- USAP Information Security Awareness training is a federal requirement.
- NSF and USAP information security policies are available on the Internet.
- Immediately report actual or suspected information security incidents, or any incidents of suspected fraud, waste, or misuse to the Denver IT Help Desk.
- When using USAP resources for work related activities and personal use, go beyond the stated rules of the USAP Enterprise Rules of Behavior (EntROB), and use your best judgment and highest ethical standards to guide your actions.
- Do not use P2P applications unless specifically authorized by the NSF for legitimate official business purposes.
- Violation of copyright laws is considered an illegal activity, and is not tolerated on the USAP network.
- Follow USAP IT best practices for password protection, system maintenance, physical security, and web and email use.
- USAP-provided equipment that transmits or receives data is the property of the NSF and is subject to monitoring.

- You are responsible for what you post on the Internet and communicate via email. Do not transmit material that may be interpreted as an adverse activity, or as hostile material.
- Acceptable recreational uses of USAP resources may be limited or restricted if necessary to support mission-critical work.
- All USAP participants are responsible for recognizing sensitive information (SI) and avoiding inappropriate access, use, or disclosure.
- Encrypt USB drives, laptops, smart phones, and mobile devices that have authorized and required sensitive information (SI).
- Remove USAP sensitive information (SI) from portable devices if it is not authorized and required for the USAP mission.

United States Antarctic Program
INFORMATION SECURITY AWARENESS
Concept Review

Answer the following questions to challenge your understanding of USAP Information Security. For your reference the correct answers are provided on pages 4-6.

1. What is PII?
    a. Information about a federal agency that is publicly available.
    b. Information about an individual maintained by an agency that can be used to distinguish or trace an individual's identity.
    c. Paper documents maintained by a federal agency.
    d. Information on U.S. citizens who have a U.S. passport.
2. Where can you find USAP Information Security policies?
    a. The Technology section of the USAP website (www.usap.gov).
    b. USAP Information Security policies are not publicly available.
    c. Policies are presented when you log on to the USAP network.
    d. The USAP McMurdo Station intranet.
3. What forms of communication are subject to monitoring?
    a. USAP-provided email.
    b. USAP-provided smart phones and mobile devices.
    c. Recreational Internet use.
    d. All of the above.
4. Which of the following are examples of deceptive Internet practices?
    a. Theft of a mobile device or shoulder surfing.
    b. Password protection, system maintenance and physical security.
    c. Misspelled URLs linked to forged web sites, unsolicited emails and instant messages.
    d. Copyright infringement.
5. What Internet activities may be interpreted as interfering with or negatively impacting the USAP mission?
    a. Discussing the effectiveness of USAP processes, facilities, or funding in a public forum.
    b. Distributing proprietary information about USAP operations to unauthorized individuals.
    c. Posting a blog of your experiences while deployed to Antarctica.
    d. A and B.

6. Which of the following is a best practice for managing sensitive information?
    a. Provide personal information on all USAP participants to anyone who inquires.
    b. Only transmit PII via email if the data is encrypted.
    c. Store records containing sensitive information on network drives with access limited to individuals who require access to perform a legitimate function.
    d. When no longer required, dispose of paper documents and electronic media containing sensitive information via public waste disposal mechanisms.
    e. B and C only.
7. What are USAP IT best practices?
    a. Password protection, system maintenance, physical security, and proper web and email use.
    b. Transmitting classified information, streaming media, network gaming over the Internet, and hosting a chat room or personal email server.
    c. Election material, personal encryption of transmissions, and installing third-party software on USAP systems.
    d. Recreational Internet use for online banking, shopping, and personal email.
8. In which of the following cases should you contact the IT Help Desk?
    a. Suspected unauthorized disclosure of PII.
    b. Loss or theft of personal or U.S. government computer equipment.
    c. If you receive an email and suspect it may be an attempt at identify theft or some other malicious activity.
    d. All of the above are potential information security incidents to immediately report to your local IT Help Desk.
9. The USAP logon banner is a reminder of what?
    a. You have no expectation of privacy in anything you do on your computer when it's connected to the USAP network.
    b. You can expect privacy if you log in to the USAP network from home or from your dormitory room on station.
    c. Others in the USAP may use your login information.
    d. You should contact USAP Information Security personnel with questions to find out more how you can help maintain a secure environment.

10. Before connecting a computer to the USAP network, what needs to occur?
    a. Nothing. It is safe to immediately connect any computer to the USAP network.
    b. You should make sure the antivirus software is up-to-date and enabled to auto-update.
    c. You should apply all relevant patches.
    d. You should properly maintain your system by performing both B and C.
11. In the media download scenario, Bob notices that network bandwidth is negatively impacted by recreational downloading of media files. What is the best course of action for Bob to lower the impact of recreational Internet activity on the USAP mission?
    a. Bob should come back to the kiosk during off-duty hours and at a time when less people are downloading files.
    b. Bob should stop using the Internet while on the Ice.
    c. Assuming grantees get preferential bandwidth for personal use, Bob should go to the science lab and download the media files he is interested in.
    d. Bob should ask someone else in the kiosk area to download files for him while he downloads other files.
12. Why is using Skype prohibited on the USAP network?
    a. Skype is peer-to-peer software that uses proprietary software and protocols.
    b. Skype is a Trojan software program.
    c. Skype does not meet federal information security requirements.
    d. A and C.
13. What activities may be interpreted as hostile material?
    a. Making threats, sexual remarks, or using hate speech in text messages or email.
    b. Posting false statements or gossip on a web site to humiliate someone.
    c. Disclosing someone's personal data (real name, address, or workplace/schools) on a web site or forum without the person's consent.
    d. All of the above.
14. Bandwidth available at McMurdo Station is equivalent to which of the following examples?
    a. The amount available to a typical office building.
    b. The amount available to one household serviced by a cable modem.
    c. The amount available by an Internet service provider to a mid-sized city.
    d. There is no Internet access at McMurdo Station.

United States Antarctic Program
INFORMATION SECURITY AWARENESS
Concept Review

Review Your Answers

1. What is PII?

   Correct answer: b Information about an individual maintained by an agency that can be used to distinguish or trace an individual's identity.

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

2. Where can you find USAP Information Security policies?

   Correct answer: a The Technology section of the USAP website (www.usap.gov).

   The USAP web site also has information on computer requirements for laptop screening and vulnerability scanning.

3. What forms of communication are subject to monitoring?

   Correct answer: d All of the above. (USAP-provided email, USAP-provided smart phones and mobile devices, and recreational Internet use.)

   If you prefer not to have your personal communications subject to monitoring, use a web-based mail service, and do not store personal messages or files on USAP network or desktop storage systems, or on USAP-provided devices.

4. Which of the following are examples of deceptive Internet practices?

   Correct answer: c Misspelled URLs linked to forged web sites, unsolicited emails and instant messages.

   The goal behind deceptive Internet practices is to corrupt your system or steal personally identifiable information (PII) that may be used to compromise personal financial resources.

5. What Internet activities may be interpreted as interfering with or negatively impacting the USAP mission?

   Correct answer: d A and B (Discussing the effectiveness of USAP processes, facilities, or funding in a public forum, and distributing proprietary information about USAP operations to unauthorized individuals.)

   Avoid making statements that are contradictory to USAP mission or NSF objectives in a public forum.

6. Which of the following is a best practice for managing sensitive information?

   Correct answer: e B and C only (Only transmit PII via email if the data is encrypted, and store records containing sensitive information on network drives with access limited to individuals who require access to perform a legitimate function.)

7. What are USAP IT best practices?

   Correct answer: a Password protection, system maintenance, physical security, and proper web and email use.

8. In which of the following cases should you contact the IT Help Desk?

   Correct answer: d All of the following are potential information security incidents to immediately report to your local IT Help Desk. (Suspected unauthorized disclosure of PII, loss or theft of personal or U.S. government computer equipment, if you receive an email and suspect it may be an attempt at identify theft or some other malicious activity.)

9. The USAP logon banner is a reminder of what?

   Correct answer: a You have no expectation of privacy in anything you do on your computer when it's connected to the USAP network.

10. Before connecting a computer to the USAP network, what needs to occur?

    Correct answer: a You should properly maintain your system by performing both B and C. (You should make sure the antivirus software is up-to-date and enabled to auto-update, and apply all relevant patches.)

11. In the media download scenario, Bob notices that network bandwidth is negatively impacted by recreational downloading of media files. What is the best course of action for Bob to lower the impact of recreational Internet activity on the USAP mission?

    Correct answer: a Bob should come back to the kiosk during off-duty hours and at a time when less people are downloading files.

12. Why is using Skype prohibited on the USAP network?

    Correct answer: d A and C (Skype is peer-to-peer software that uses proprietary software and protocols and Skype does not meet federal information security requirements.)

    Also, Skype transmissions cannot be decrypted, which can lead to the spread of Viruses, SpyWare, Trojan horses, and can compromise your privacy.

13. What activities may be interpreted as hostile material?

    Correct answer: d All of the above. (Making threats, sexual remarks, or using hate speech in text messages or email, posting false statements or gossip on a web site to humiliate someone, disclosing someone's personal data (real name, address, or workplace/schools) on a web site or forum without the person's consent.)

    When using USAP resources for work related activities and personal use, go beyond the stated rules of the USAP Enterprise Rules of Behavior (EntROB), and use your best judgment and highest ethical standards to guide your actions. Taking this precaution assures that your activities are not interpreted as hostile material.

14. Bandwidth available at McMurdo Station is equivalent to which of the following examples?

    Correct answer: b The amount available to one household serviced by a cable modem.

    During the austral summer season at McMurdo when over 1,000 people are sharing this resource, it is essential that available bandwidth is primarily dedicated to operational and science support requirements. Acceptable recreational uses of USAP resources may be limited or restricted if necessary to support mission-critical work.