The National Science Foundation
Polar Programs
United States Antarctic Program

Information System Rules of Behavior ICT-INST_ 5000.24
USAP Enterprise Information Infrastructure

Organizational Function	Information Resource Management	Document Number	ICT-INST_5000.24
		Issue Date	10/20/2014
Policy Category	Information Security Policies	Effective Date	10/20/2014
		Review On	10/20/2016
Subject	Information System Rules of Behavior USAP Enterprise Information Infrastructure	Authorized By	Mr. Patrick Smith Manager, Technology Development, Polar Research Support
Office of Primary Responsibility	National Science Foundation Geosciences Directorate Division of Polar Programs Antarctic Infrastructure and Logistics	Responsible Official	USAP Information Security Manager
Address	Suite 755 4201 Wilson Blvd Arlington, VA 22230	Phone Fax Web	703.292.8032 703.292.9080 http://www.nsf.gov/div/index.jsp?div=plr
Distribution	USAP-Wide	Status	Final
Online Publication	http://www.usap.gov/technology/contentHandler.cfm?id=1563		

Document Release History

Release Number	Release Date	Description of Changes	Author	Organization
1.0	10/20/2014	Initial release as USAP instruction	Pat Smith	NSF

Table of Contents

THIS PAGE INTENTIONALLY LEFT BLANK

1 GENERAL INFORMATION

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

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

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

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

Questions. If you have any questions about these Rules, please contact the USAP Help Desk at 720-568-2001 or helpdesk@usap.gov. The responsible NSF point of contact for these Rules of Behavior is the USAP Information Security Manager, NSF Division of Polar Programs, 4201 Wilson Blvd, Suite 755, Arlington, VA 22230, 703.292.8032.

2 DEFINITION OF AN INFORMATION SYSTEM

For the purpose of the Rules of Behavior the following definitions apply:

USAP Information System - Information systems directly supporting the mission of the United States Antarctic Program; including those provided or managed by another federal agency, contractor, or other source. A USAP information system is typically procured using NSF program funds for USAP operations or have property accountability to NSF. Such systems may consist of:

a) **Government Owned Contractor Operated (GOCO) Systems** - U.S. Government owned systems where a contractor provides design, development, deployment, operations, and/or phase-out.

b) **Government Owned Government Operated (GOGO) Systems** - U.S. Government owned systems where a component of the U.S. Government provides design, development, deployment, operations, and/or phase-out.

Contractor Information System - Relevant Contractor Information Systems consist of information systems used in contract performance supporting the mission of the United States Antarctic Program that are other than incidental in nature. Such systems may consist of:

a) **Contractor Owned Contractor Operated (COCO) Systems** - Contractor owned IT systems used in the support of performance of contract activity that are other than incidental in nature pertaining to services provided to the USAP.

b) **Contractor Owned – Interconnected (CO-Int) Systems** - All contractor owned systems that are directly connected with USAP information systems (including USAP networks).

Non-USAP Information System. Systems that may or may not support the mission of the USAP. A non-USAP Information System is typically not procured using NSF program funds for USAP operations. Such systems may consist of:

a) **Science and Research Systems –** Systems connected to the USAP network in support of research to include scientific research instrumentation and transitory mobile computing devices. These systems are procured or provided directly via NSF research grants or NSF co-sponsored research grants and are operated by or for the grantee. *NB: In cases where NSF provides systems for science/research support purposes directly (e.g., via USAP operational assets or program funding), the system shall be considered a USAP Information System.*

b) **Tenant and Guest Systems –** Systems that are provided by a tenant organization or guest operating within the USAP operational environment that do not strictly fall under the other systems defined for the category "USAP" or "Non-USAP". These systems are typically provided by NSF sponsored tenants/guests via means independent of NSF in support of sanctioned official business within the USAP operating environment. Examples are other Federal agencies and contractors that self-provision equipment.

c) **Personal Use Systems –** Systems that are procured or operated by individuals principally for personal use. The owner can be any USAP participant, regardless of affiliation. *NB: For conditions of mixed used where a personally owned device is also used for official business purposes, the device shall incur any restrictions for Personal Use Systems in addition to any applicable restrictions from other relevant categories defined herein.*

3 NO EXPECTATION OF PRIVACY WHILE USING USAP INFORMATION RESOURCES

Information maintained in NSF systems, including electronic mail files, may be reviewed by NSF officials who have a legitimate reason to do so when authorized by the Director or Deputy Director, or by the Inspector General.

Users of USAP information resources have no expectation of privacy with respect to any information residing on government information systems or transmitted over government information networks, other than the regular expectations associated with information governed by the Privacy Act of 1974, as amended.

4 ACCEPTABLE USES OF USAP INFORMATION RESOURCES

The following activities are considered acceptable uses of the USAP Information Infrastructure. All users are reminded that USAP mission activities always take precedence over any personal

activity. The NSF reserves the right to restrict or otherwise limit personal use based on resource availability, conflict with official business, and unacceptable information security risks.

- **Personal Telephone and Facsimile Use.** Users may make personal telephone calls (including use of facsimile machines and voice mail). As long as it is only a minimal cost to the government. The user is responsible for charges incurred when using the infrastructure for personal use.
- **Personal Use of Electronic Mail.** 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.** Some limited personal use of Internet services is permitted, provided it does not interfere with the participant's work or the work of others and does not incur excessive use of government resources or disruption of government business and does not violate other elements of this policy.
- **Web Cameras and Collaborative Computing.** Web cameras for training, meetings, educational outreach programs, official business, or personal use is permitted according to NSF policy and with the approval of NSF.
- **Wireless**. USAP Information Technology (IT) services manages wireless access points for connecting to the USAP network. Requests for access must be made to IT staff.
- **Radio Communication**. 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 & 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. All uses of VPN & Secure Shell shall conform to all terms and condition of these enterprise rules of behavior. For further guidance see your organizational IT point of contact.

5 PROHIBITED USES OF USAP INFORMATION RESOURCES

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

- **Illegal Activities.** All illegal activities are forbidden.
- **Adverse Activities.** Any activity that could adversely affect NSF or US Government interests, interfere with the performance of the USAP mission.
- **No Processing of Classified Information.**
- **Hostile Environment.** Under no circumstances is it permissible to access or download material that would create a hostile or offensive work environment, such as racist or sexually explicit material.

Prohibited Email Activities.

a) USAP hosted email system services - Allowing others to use an assigned email account is prohibited. Placing others on a mailing list, subscription list, chat room list, or other list service without their consent is prohibited. "All employee" or broadcast messages disseminated using USAP information resources must be business related and approved in advance by the applicable manager. Using large distribution lists for non-business-related purposes is prohibited. Using USAP hosted email system services to proselytize or solicit for personal commercial ventures, religious or political causes, or outside organizations is prohibited.

b) Any email service originating within or transiting through the USAP information environment - Creating, originating, distributing or circulating “chain” or “pyramid” transmissions, mass mailings, hoaxes, spamming, phishing or harassing messages is prohibited. Sending large, memory intensive files or applications which may impede or disturb network operation is prohibited.

Personal Information Infrastructure. Personal IT infrastructure (e.g., www servers, firewalls, application servers, IP enabled systems, etc.) beyond typical consumer-grade computing devices (e.g., laptop computer) of any type are prohibited. 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, ORW, SIP, RSP, and approved 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 (see, **Representation of Identity Online**).

Representation of Identity Online. The use of USAP information resources that result in user identity displayed or documented as affiliated with the USAP (e.g., social media such as twitter, facebook, personal blog, etc, electronic mail addresses, IP network addresses, usap.gov domain name) produce the appearance of an official communication representing the National Science Foundation. Only official use is sanctioned. Unauthorized use may be subject to administrative, civil, or criminal penalties .

Mobile Code. The importation or use of unsigned mobile code is prohibited without prior written approval of the USAP Information Security Manager.

Streaming Media. Use of bandwidth intensitve streaming media services within the USAP network environment is prohibited. Typical examples are over-the-top network movie and television video streaming services, live/rebroadcast radio feeds, or on-line music feeds.

Peer-to-Peer Services and Software. Use of USAP information resources to participate in peer-to-peer networking or file sharing systems is prohibited. The installation of peer-to-peer software on devices attached to the USAP information system environment prohibited on USAP Systems and must be disabled and passivated on non-USAP systems.

Prohibited Business and Commercial Uses. Conducting non-program business activities is prohibited. Using USAP resources to advertise commercial goods or services for sale for monetary or personal gain is prohibited. Using USAP resources to conduct non-program commercial activities is prohibited. Users may not establish on maintain a web-based business at a USAP operating location.

Prohibited Network Activities. Knowingly downloading, installing, storing or using malicious software, viruses, "cracking," keystroke monitoring software or hardware, port scanners, vulnerability scanning, penetration tools, circumvention of system security features, intentional acts to exceed security authorizations, attaching unauthorized equipment to networks or other actions that may be disruptive, expose USAP information systems to cybersecurity risks or counter-productive to business operations is prohibited. The introduction or use of packet sniffing software or any software intended to capture passwords is prohibited. Monitoring network traffic (e.g., run a sniffer); unauthorized access of IT infrastructure; or copying data, files, or software without prior authorization is prohibited.

Prohibited VPN & Secure Shell. Unofficial personal virtual private networks (VPNs) and Secure Shell services are explicitly prohibited from connecting to the USAP network. Any VPN that is not authorized and registered in advance by USAP Information Technology (IT) services is prohibited, whether or not for business purposes. NSF establishes the criteria and issues final judgment to distinguish between official and unofficial determination.

Identity cloaking. Software or tools as web traffic anonymizers or any identity cloaking software are strictly prohibited and may be disconnected or blocked without notice.

Prohibition on Tampering. Unless explicitly authorized by NSF designated personnel, individuals using NSF/USAP information systems and services do not have permission to physically access, modify, interconnect or alter configuration settings or in any way change or disrupt any information system or network infrastructure (data centers, servers, embedded systems, telephone systems, wiring closets, network port outlets, frame rooms, cable plant other than accessing designated outlets, etc.). Users are not allowed to attach any unauthorized device to any USAP network infrastructure. Individuals found to be in violation of this prohibition may be subject to appropriate administrative sanctions, civil liability or criminal prosecution.

Wireless. Wireless access points that connect to the USAP network are officially managed. Requests for access must be made to IT staff. Attaching end-user provided wireless access point equipment to USAP information infrastructure is prohibited unless specifically authorized by NSF. Unauthorized equipment shall be blocked without notice, disconnected and confiscated. Confiscated equipment will only be returned to the owner upon departure from the USAP operating location.

6 ADDITIONAL GUIDANCE FOR USERS

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

- Comply with these Rules of Behavior and all other NSF/USAP policies and procedures, as well as the policies and procedures of their sponsoring organization
- Protect sensitive information from unauthorized disclosure. The determination of sensitive information disclosure is the sole authority of NSF.
- Ensure information security through effective use of user IDs and passwords
- Protect hardware, software, and information from damage, abuse, and unauthorized use
- Report security violations and vulnerabilities to the proper authorities. The Help Desk is the first point of contact for all reports
- Users shall not leave an active system unattended, thereby allowing an unauthorized person to gain access to a network or a computing system through the user's login session
- Users are responsible to ensure the integrity, availability, and confidentiality of all U.S. Government work-related data on systems assigned for their use. It is recommended that critical data on a hard disk be backed up periodically.

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

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

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

Personal File Storage. Each user is typically assigned a 'home' directory on their primary network which is usually accessible from any computer. This drive is provided for the storage of files associated with the user's network credentials. Files stored in this directory are not considered private, but will be afforded the same management regarding disclosure as defined in NSF agency policy.

Common File Storage. At each operating location, one or more directories are established for common use, and are accessible to all users. A temporary directory is provided for temporary (less than one week) use by users. Users have full rights to this directory and may add or delete files and directories as needed. All files and directories in the temporary directory are deleted

automatically once a week, on a schedule determined by the local IT staff. A permanent common area is intended for operational storage and use. Users typically have read-only rights to this directory. Content stored must conform to the stipulations set forth in these Rules regarding acceptable and prohibited use.

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

Security of Equipment on the USAP Network. All equipment on the network is subject to interconnection standards, software security compliance patch compliance, vulnerability scanning and remediation. USAP participants are responsible for remediating vulnerabilities detected on their equipment. Laptops and other portable computing devices, such as Personal Digital Assistants, tablet computers, "smart" phones, and scientific /research instrumentation systems must be evaluated for compatible software and up-to-date anti-virus protection before they are used on the USAP network. All users of USAP information resources must comply with USAP policies regarding the use of antivirus software.

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

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

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

Wireless. Wireless networks should not be used as a substitute for wired network connections as much as practicable. Whenever possible a physical port connection to the network should be used. Exceptions may be considered if additional security controls are in place, and the request is approved in advance by the U.S. Antarctic Program Information Security Manager (USAP ISM).

Sensitive Information. Sensitive information must be properly handled. Sensitive information includes: medical, acquisition, operational security, commercial/proprietary, information security, and privacy data. USAP information resource users must acquire and use sensitive information only in accordance with established policies and procedures. This includes properly safeguarding sensitive information contained in hardcopy or softcopy; ensuring only those with a need to know have access, and ensuring sensitive information is accurate, timely, complete, and relevant for the purpose which it is collected, provided, and used.

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

7 ADDITIONAL GUIDANCE FOR CONTENT PROVIDERS AND SYSTEMS ADMINISTRATORS

Auditing of Information Systems. Information Technology, communications, and security personnel will regularly review telecommunications logs, text message logs, phone records, and conduct spot-checks to assess user compliance with controls placed on the use of USAP information resources.

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