THE NATIONAL SCIENCE FOUNDATION

Office of Polar Programs

United States Antarctic Program

AIL-POL-5000.06 Effective Date: January 2020

Acceptable Use of USAP Information Resources Review Date: January 2025

Short, Stephanie A. Digitally signed by Short, Stephanie A.
Date: 2020.01.09 17:58:53 -05'00'

Stephanie A. Short Date
Section Head, Antarctic Infrastructure and Logistics
U.S. Antarctic Program Authorizing Official
Office of Polar Programs

1.0 PURPOSE

This directive establishes the acceptable use policy for the National Science Foundation (NSF) United States Antarctic Program (USAP). The USAP is managed by the Office of Polar Programs (OPP). The purpose of this policy is to define acceptable personal use of USAP technology and communication resources. This directive supplements the NSF *Information Security Handbook, Manual 7*, and addresses the applicable controls noted in NIST Special Publication (SP) 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

This directive updates the following OPP policies and supporting documents:

- Replaces USAP Information Resource Management Directive 5000.6, Acceptable Use of USAP Information Resources with this policy;
- Replaces USAP Enterprise Information Infrastructure Instruction 5000.24, Information System Rules of Behavior with Appendix A of this policy;
- Updates content for ICT_FRM-5000.24a, *Acknowledgement of Information Security Policies and Permission for Use of National Science Foundation/United States Antarctic Program Information Systems and Services* (Appendix A);
- Updates content for ICT_FRM-5000.24b, *Acknowledgement of United States Antarctic Program Rules of Behavior for Sensitive Information and Personally Identifiable Information* (Appendix B).

2.0 SCOPE

This policy covers all USAP technology and communication resources within the USAP operating environment or connected to the USAP information infrastructure and applies to everyone who uses them. USAP information technology and communications resources include:

- Internet access and electronic mail systems

- Telephones, radios, pagers, and other telecommunications devices and services for receiving and transmitting voice and/or data, to include voice mail
- Computer hardware, software, and other office equipment, including copiers and fax machines
- Records and other similar materials related to USAP activities and operations

This policy also applies to users who may need to access NSF information technology and communications resources as part of their USAP activities.

3.0 GUIDING PRINCIPLES

In establishing practices for acceptable use within the USAP, OPP will follow these guiding principles:

- USAP information resources, especially at the Antarctic research stations and aboard the research vessels, may be used for certain personal uses in a manner that does not interfere with the program's mission. All mission activities take precedence over personal activities at all times.
- Systems and network administrators, and others who may be exposed to a participant's personal communications as a part of their normal duties, are in a position of trust and will be held accountable for violations of that trust on their part.
- OPP is not a common carrier and does not possess the requisite infrastructure and resources necessary to guarantee the privacy of information processed or stored on USAP information systems or networks. By their use of any USAP information system users of USAP systems agree that the government and its representatives are not responsible for the loss of personal information, or for the disclosure of personal information as a result of unauthorized activity by participants or by others outside the program.
- Participants and their leaders are expected to use good judgment in appropriate use of program assets consistent with the purposes of this policy. The final determination regarding what constitutes appropriate use consistent with this policy is reserved to OPP management in coordination with the participant's organization.

4.0 DEFINITIONS

4.1 Official Business

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

4.2 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.

4.3 Rules of Behavior

OPP has established the Enterprise Rules of Behavior (EntRoB) and the Sensitive Rules of Behavior (SenRoB) for USAP participants to follow at all times. These are provided in the Appendix to this policy. Additional USAP applications may have Rules of Behavior specific to that application.

5.0 POLICY

All users of USAP information systems shall adhere to the NSF Acceptable Use Policy, which is published in NSF Bulletin No. 13-06, *Personal Use Policy for NSF Technology and Communication Resources*. NSF Bulletin 13-06 is included in Appendix C of this policy for ease of reference.

All users of USAP information systems shall adhere to the NSF Policy for Social Media Use when using social media in their USAP activities. The NSF Policy for Social Media is published in NSF Staff Memorandum OD 19-12, *Policy for Social Media Use*, and is included in Appendix D of this policy for ease of reference.

To supplement the NSF acceptable use policies for personal use and social media and to address operational needs specific to the USAP, OPP has published the USAP Enterprise Rules of Behavior (Appendix A) and the USAP Sensitive Rules of Behavior (Appendix B). OPP may also establish Rules of Behavior for specific USAP information systems and applications as needed.

All users of USAP information technology resources shall adhere to the USAP Enterprise and Sensitive Rules of Behavior and any system or application Rules of Behavior at all times.

All users must acknowledge, in writing or other verifiable means, that they have received the Rules of Behavior and consent to follow the rules.

Users of the Participant On-Line Antarctic Resource Information Coordination Environment (POLAR ICE) must acknowledge the POLAR ICE Rules of Behavior before using the system the first time and annually thereafter, a copy of which is retained in the system.

Acknowledgement must be completed before the user is allowed to access any USAP information system, and every year thereafter while the user maintains access to the USAP information system.

Personnel with responsibilities for protecting sensitive information, such as personally identifiable information (PII) must acknowledge and adhere to the Sensitive Rules of Behavior prior to accessing sensitive information and annually thereafter.

Occasional personal use of NSF USAP-supplied technology and communication resources is allowed when the cost to the government is negligible and the personal use does not interfere with official business, provided that the following criteria are met:

- any personal use of the agency’s property is subject to the overriding expectation that employees will give the government a full day’s labor for a full day’s pay
- employees are responsible for making it clear that they are not acting in an official capacity when they are using technology and communication resources for personal purposes
- the use is not for personal gain (See, NSF Manual 15, Conflicts of Interest and Standards of Ethical Conduct).
- the use does not create a security risk for NSF (See, Security and Privacy Awareness training)

- as part of a user's mandatory annual Security and Privacy Awareness training, users agree to NSF and USAP Rules of Behavior. These rules prohibit users from seeking, transmitting, collecting, or storing:
  - defamatory, discriminatory, harassing, or intimidating material that could discredit NSF or damage its public reputation
  - obscene or pornographic material.
- the use is not offensive to coworkers
- the use is not for illegal activities, such as the distribution of copyrighted materials or media
- the use is not for gambling and on-line auctions

Specifically with regard to telecommunications services the use must not violate the Federal executive order (EO 13513) forbidding Federal employees to send text messages while driving.

Users should be aware that:

- they have no expectation of privacy when using government-provided access to the Internet or electronic mail systems
- files maintained in NSF USAP equipment and systems, including electronic mail files, may be reviewed by NSF officials who have a legitimate reason to do so when authorized by the NSF Director, Deputy Director, or by officials in the Office of Inspector General
- electronic mail messages and other records maintained in NSF USAP equipment and systems may be made available to the public under provisions of the Freedom of Information Act
- NSF reserves the right to prevent access from USAP devices to Web sites determined to be inappropriate or illegal
- unauthorized persons, such as family members, are not allowed to use NSF USAP technology and communication resources

NSF officials or a user's USAP manager may limit or revoke personal use of agency resources for any business reason.

Any use of USAP information resources not covered in this policy must be authorized by OPP.

6.0 INFORMATION SECURITY CONTROLS

NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations* includes security controls for Acceptable Use of federal information systems. This section states the OPP policy for implementing these controls within the USAP.

PL-4 RULES OF BEHAVIOR

For the USAP, OPP shall:
a. Establish and make readily available to USAP participants requiring access to USAP information systems, the rules that describe their responsibilities and expected behavior with regard to information and information system usage;
b. Receive a signed acknowledgment from such individuals, indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to USAP information and the information system;
c. Review and update the rules of behavior annually; and

d. Require individuals who have signed a previous version of the rules of behavior to read and re-sign when the rules of behavior are revised/updated.

PL-04(1) RULES OF BEHAVIOR | SOCIAL MEDIA AND NETWORKING RESTRICTIONS

For the USAP, OPP shall include in the Rules of Behavior explicit restrictions on the use of social media/networking sites and posting USAP information on public websites.

USAP participants shall sign the Rules of Behavior to acknowledge they are accountable for their use of social media sites.

7.0 ROLES AND RESPONSIBILITIES

The *NSF Information Security Handbook Manual 7* defines the governance structure for the NSF Information Security and Privacy Program. For the USAP, OPP supplements the NSF governance structure as follows:

7.1 USAP Authorizing Official

The USAP Authorizing Official (AO) is the OPP senior executive with the authority to formally assume responsibility and accountability for operating the USAP information systems. The USAP AO is the OPP official designated by the NSF Chief Information Officer who can accept the security and privacy risk to USAP operations, assets, and individuals. The USAP AO ensures compliance with applicable NSF information security and privacy requirements, develops and evaluates USAP information security and privacy policy, and manages USAP information security and privacy risks.

7.2 USAP Information Security Manager

The USAP Information Security Manager (ISM) provides oversight for the implementation of information security and privacy controls for USAP information systems and coordinates within OPP and with the NSF Division of Information Systems for matters concerning the acceptable use of NSF USAP information systems.

7.3 Antarctic Support Contract

The Antarctic Support Contract (ASC) is the contract through which OPP operates and maintains the information technology and communications (ITC) systems that support the USAP mission and business functions. The ASC prime contractor executes the contract for OPP and implements the information security and privacy policies for the USAP to include enforcement of controls to manage use of USAP information systems and block prohibited activities.

7.4 USAP Participating Organizations

Members of participating organizations that have the need to access USAP information ensure their use adheres to the NSF and USAP Rules of Behavior at all times.

8.0 ENFORCEMENT

Failure to comply with information security and privacy policies may result in disciplinary action.

9.0 REVIEW

This policy is valid until rescinded. It will be reviewed at an interval of not more than 5 years.

10.0 AUTHORITY

The USAP Authorizing Official approves this policy. The policy aligns with the authority of the NSF Act of 1950 and NSF guidance regarding the security and privacy of information and information systems and the protection of sensitive information, including PII.

11.0 REFERENCES

- NSF Act of 1950, 42 U.S.C. §1861 et seq., PL 81-507, May 1950
- The Privacy Act of 1974, 5 U.S.C. § 552a
- Federal Information Security Modernization Act of 2014 (FISMA) 44 U.S.C. §3551 et seq., PL 113-283, December 2014
- OMB Circular A-130, *Managing Information as a Strategic Resource*
- OMB M-06-16, *Protection of Sensitive Agency Information*
- OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*
- OMB M-20-04, *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements*
- NIST Special Publication 800-53, Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
- NSF *Information Security Handbook Manual 7*
- NSF Staff Memorandum OD 19-12, *Policy for Social Media Use*
- NSF *IT Security and Privacy Awareness Training Rules of Behavior*
- NSF Bulletin 13-06, *Personal Use Policy for NSF Technology and Communication Resources*

DOCUMENT REVISION HISTORY

Version	Date	Changes	Author
0.0	8/4/2004	Initial publication of policy	NSF/OPP
1.0	6/9/2011	Update to 800-53 rev 2	NSF/OPP
2.0	5/3/2012	Update	NSF/OPP
3.0	5/11/2013	Update to 800-53 rev 3	NSF/OPP
4.0	12/20/2019	Update to policy to align with NIST 800-53 Rev 4 and NSF Information Security Handbook.	NSF/OPP
4.0	1/9/2020	Final for signature and publication	NSF/OPP

APPENDIX A USAP ENTERPRISE RULES OF BEHAVIOR

All USAP participants and any other person who uses USAP information systems or otherwise access USAP information shall review and acknowledge the USAP Enterprise Rules of Behavior before being granted access, and at least annually thereafter while they have access to the USAP information systems. Acknowledgement may be accomplished by electronic means or by completing ICT_FRM_5000.24a, Acknowledgement of Information Security Policies and Permission for Use of National Science Foundation/United States Antarctic Program Information Systems and Services or as otherwise approved by OPP. This section presents the USAP Enterprise Rules of Behavior, which are also available online at www.usap.gov.

1 GENERAL INFORMATION

The National Science Foundation (NSF) Office of Polar Programs (OPP) provides information systems for the purpose of transacting the official business of the U.S. Antarctic Program (USAP). 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 OPP. 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 Office of Polar Programs, 2415 Eisenhower Avenue, Alexandria, Arlington, VA 2231422230, 703.292.8032.

2 DEFINITIONS 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 intensive 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.

8 ADDITIONAL GUIDANCE ON THE OF SOCIAL MEDIA/NETWORKING SITES AND POSTING ORGANIZATIONAL INFORMATION ON PUBLIC WEBSITES.

"Social media" is a general term that encompasses Web tools for online collaboration and information sharing. These tools include, but are not limited to, technologies such as blogs (e.g., WordPress, Tumblr, Medium), wikis (e.g., Wikipedia), social networks (e.g., LinkedIn, Facebook, Twitter, Instagram), file sharing sites (e.g., Flickr, YouTube), social bookmarking and news sites (e.g., Digg, StumbleUpon, Pinterest), and virtual worlds (e.g., Second Life).

Social media is a core part of NSF's communications to the public, the research community and other interested parties, underpinning our work and advancing our mission at NSF. USAP participants are encouraged to use social media tools to enhance communication, collaboration, and information sharing in support of the USAP mission.

Use of social media must comply with the NSF Policy for Social Media Use, which applies to all USAP participants, including participants participating on the agency's behalf through official NSF social media platforms and participants with personal accounts who identify themselves as USAP participants.

When using social media, USAP participants are expected to exercise decorum and professionalism and to comply with all relevant NSF and USAP policies.

If accessing social media for personal purposes while at work, employees must comply with the NSF and USAP acceptable use policies, to include these Rules of Behavior. For more information see the NSF Policy on Social Media Use in Appendix D of AIL Policy 5000.06, Acceptable Use of USAP Information Resources.

APPENDIX B USAP SENSITIVE RULES OF BEHAVIOR

All USAP participants and any other person who uses USAP information systems or otherwise access USAP information and have need to access or may encounter sensitive information, to include personally identifiable information (PII) shall review and acknowledge the USAP Sensitive Rules of Behavior before being granted access, and at least annually thereafter while they have access to the USAP information systems. Acknowledgement may be accomplished by electronic means or by completing ICT_FRM_5000.24b, Acknowledgement of United States Antarctic Program Rules of Behavior for Sensitive and Personally Identifiable Information or as otherwise approved by OPP. This section presents the USAP Sensitive Rules of Behavior, which are also available online at www.usap.gov.

1. GENERAL INFORMATION

The purpose of the United States Antarctic Program (USAP) Rules of Behavior for Sensitive Information (SI) and Personally Identifiable Information (PII) is to highlight federal laws and guidelines from NSF and other federal documents for USAP participants with access to SI or PII.

Sensitive Information is information that has been characterized in accord with Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information System and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-60, Guide to Mapping Information and Information Systems to Security Categories as requiring access restrictions and protection from unauthorized disclosure. Basic types include:

- Privacy Act Systems of Records
- Personal medical information (PHI – Protected health information)
- Personally Identifiable Information (PII)
- Financial Information
- Trade Secrets Act protected data
- Commercial proprietary data
- Operational Security (OPSEC) information
- Current US Air Force and Air National Guard flight operations details
- IT infrastructure information
- Detailed internal USAP network diagrams
- Information Technology information
- Root or system administrator passwords to systems on the USAP network
- Vulnerability scan results
- System log files

Personally Identifiable Information. Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*, defines PII as follows: ‘Personally identifiable information’ means information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual.

PII examples provided by NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* include but are not limited to:

- Name, such as full name, maiden name, mother's maiden name, or alias
- Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, or financial account or credit card number
- Address information, such as street address or email address
- Personal characteristics, including photographic image (especially of face or other identifying characteristic), fingerprints, handwriting, or other biometric data (e.g., retina scan, voice signature, facial geometry)
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information)

Federal laws and guidelines pertaining to SI and PII include

- The Privacy Act of 1974, 5 U.S.C. § 552a
- E-Government Act of 2002, 44 U.S.C 3601 et seq.
- Federal Information Security Modernization Act of 2014 (FISMA), 44 U.S.C. §3551 et seq., PL 113-283, December 2014
- NIST 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
- OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication Under the Privacy Act*
- OMB Circular A-130, *Managing Information as a Strategic Resource*
- OMB M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*
- OMB M-06-16, *Protection of Sensitive Agency Information*, June 2006
- OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*
- OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*
- OMB M-20-04, *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements*

The USAP Rules of Behavior for Sensitive Information and Personally Identifiable Information (SenROB) must be reviewed and signed by USAP participants with access to SI or PII. Signatories accept that they understand and take personal responsibility for the security of sensitive information and personally identifiable information.

The USAP SenROB is founded on the principles described in federal law, and other regulatory documents such as the Code of Ethics for Government Employees, Office of Personnel Management regulations, and Office of Management and Budget. Therefore, the SenROB carries the same responsibility for compliance as the official documents cited above.

2. USER RESPONSIBILITIES

In the course of performing official duties, USAP participants with access to SI or PII are responsible for avoiding inappropriate access or disclosure of SI and PII of any kind and are bound to follow certain methods of storage and transmission for these kinds of data. These rules of behavior detail the responsibilities of and expectations for all individuals with access to SI and PII.

3. RESPONSIBILITY/ACCOUNTABILITY REQUIREMENTS

Users should only use systems, software, and data for which they have authorization and use them only for official USAP business.

Users with access to systems and data that utilize SI or PII must view and access this information only for the purposes for which use of the data is intended.

Users must protect sensitive information from unauthorized disclosure.

Users shall not store SI or PII on portable devices such as laptops, tablets, smart phones and USB drives or on remote/home systems unless approved encryption methods are employed.

Users are prohibited from transmitting SI or PII via plain text email; only approved encryption methods shall be used.

All records containing SI or PII must be stored on network drives with access limited to those individuals or entities that require access to perform a legitimate job function.

All removable or transportable media (e.g. paper forms, reports, cassettes, CDs, USB drives, etc.) containing SI or PII must be secured when not in use. Acceptable security measures depend on the circumstances, but may include locked file rooms, desks, cabinets and encryption.

Subject to applicable document retention policies or unless required by law, when no longer required, paper documents and electronic media containing SI or PII must be destroyed or disposed of using methods designed to prevent subsequent use or recovery of information in accordance with NIST SP 800-88, Guidelines for Media Sanitization and applicable USAP policy and procedures. Organizations must follow their media sanitization procedures.

In accordance with OMB Memorandum 07-16, and NSF policy, users must immediately report actual and potential incidents of inappropriate disclosure of SI or PII to the USAP Help Desk Toll Free at 1.800.688.8606 (Extension 32001) or 720.568.2001 within 24 hours of detection.

USAP participants who have access to SI or PII must adhere to these rules and guidelines.

APPENDIX C PERSONAL USE POLICY FOR NSF TECHNOLOGY AND COMMUNICATION RESOURCES

This section presents the Personal Use Policy for NSF Technology and Communication Resources, as published in NSF Bulletin No. 13-06, *Personal Use Policy for NSF Technology and Communication Resources*.

1. Scope

This policy covers all NSF technology and communication resources and applies to everyone who uses them.

NSF technology and communications resources include:

- Internet access and electronic mail systems
- Telecommunications devices and services for receiving and transmitting voice and/or data,
- Hardware, software, and other office equipment, including copiers and fax machines

2. Purpose

The purpose of this policy is to define acceptable personal use of NSF technology and communication resources.

3. Policy

Occasional personal use of NSF-supplied technology and communication resources is allowed when the cost to the government is negligible and the personal use does not interfere with official business, provided that the following criteria are met:

- any personal use of the agency's property is subject to the overriding expectation that employees will give the government a full day's labor for a full day's pay
- employees are responsible for making it clear that they are not acting in an official capacity when they are using technology and communication resources for personal purposes
- the use is not for personal gain (See, NSF Manual 15, Conflicts of Interest and Standards of Ethical Conduct).
- the use does not create a security risk for NSF (See, Security and Privacy Awareness training)
- as part of a user's mandatory annual Security and Privacy Awareness training, users agree to NSF Rules of Behavior. These rules prohibit users from seeking, transmitting, collecting, or storing:
    - defamatory, discriminatory, harassing, or intimidating material that could discredit NSF or damage its public reputation
    - obscene or pornographic material.
- the use is not offensive to coworkers
- the use is not for illegal activities, such as the distribution of copyrighted materials or media
- the use is not for gambling and on-line auctions

Specifically with regard to telecommunications services the use must not violate the Federal executive order (EO 13513) forbidding Federal employees to send text messages while driving. Employees who travel internationally are responsible for reviewing NSF's policy on reimbursement for telecommunications charges while traveling (NSF Bulletin 07-06).

Users should be aware that:

- they have no expectation of privacy when using government-provided access to the Internet or electronic mail systems
- files maintained in NSF equipment and systems, including electronic mail files, may be reviewed by NSF officials who have a legitimate reason to do so when authorized by the NSF Director, Deputy Director, or by officials in the Office of Inspector General
- electronic mail messages and other records maintained in NSF equipment and systems may be made available to the public under provisions of the Freedom of Information Act
- NSF reserves the right to prevent access to Web sites determined to be inappropriate or illegal
- unauthorized persons, such as family members, are not allowed to use NSF technology and communication resources

The general standards of employee conduct remain in effect and are outlined in NSF Manual 15 Conflicts of Interest and Standards of Ethical Conduct. A supervisor may limit or revoke personal use of agency resources for any business reason.

This personal use policy is part of a range of information technology policies for acceptable use of agency resources. NSF staff should refer to these policies for additional information.

4. Enforcement

Violation of this policy could result in disciplinary action up to and including removal and/or civil or criminal penalties, including personal financial liability for the cost of improper use.

APPENDIX D NSF POLICY FOR SOCIAL MEDIA USE

USAP Participants shall follow the NSF Policy for Social Media Use when using social media in their USAP activities. This section presents the NSF Policy for Social Media, as published in NSF Staff Memorandum OD 19-12, *Policy for Social Medial Use*. Where applicable, information specific to USAP participants is noted here.

1. Scope

This policy applies to all NSF employees, contractors, Intergovernmental Personnel Act (IPA) assignees, and Visiting Scientists, Engineers, and Educators (VSEEs), as well as fellows and interns. Hereafter, all personnel are called "employees." This policy also applies to others who have access to NSF equipment, computing services, or communication systems.

The scope of this policy includes all USAP participants.

2. Purpose

This document establishes policy for the use of social media by NSF employees in the course of their employment. This policy will evolve as new technologies and social media tools become available.

Employees are cautioned that social media distribute messages universally, in a forum accessible by all; these media create new opportunities for engagement and create new vulnerabilities. An employee's freedom to use social media brings a commensurate requirement that these media be used responsibly, mindful always that a federal employee occupies a position of public trust.

This policy builds upon longstanding NSF policies for appropriate use of information technology (IT) resources and ethical conduct while allowing NSF to use innovative technology to enhance the agency's engagement with external communities.

3. Definition

"Social media" is a general term that encompasses Web tools for online collaboration and information sharing. These tools include, but are not limited to, technologies such as blogs (e.g., WordPress, Tumblr, Medium), wikis (e.g., Wikipedia), social networks (e.g., LinkedIn, Facebook, Twitter, Instagram), file sharing sites (e.g., Flickr, YouTube), social bookmarking and news sites (e.g., Digg, StumbleUpon, Pinterest), and virtual worlds (e.g., Second Life).

4. Policy

NSF employees are encouraged to use social media tools to enhance communication, collaboration, and information sharing in support of NSF's mission. These standards apply to employees participating on the agency's behalf through official NSF social media platforms and employees with personal accounts who identify themselves as NSF employees. Employees are expected to exercise decorum and professionalism and to comply with all relevant agency policies.

If accessing social media for personal purposes while at work, employees must comply with NSF's Personal Use Policy for NSF Technology and Communication Resources, and IT Security and Privacy Policies.

Employees who create, contribute to, or participate in social media on NSF's behalf or identify themselves as NSF employees must follow the directives outlined in Section 4.1 and Section 4.2. The social media best practices described in Section 4.3 are provided as guidance only.

4.1. Social Media Use on NSF's Behalf

When using social media on NSF's behalf (on an official NSF platform2), employees must:

- Know and comply with NSF's policies for acceptable use of IT resources and standards for ethical conduct. IT policies and other pertinent information can be accessed from the IT Security and Privacy Policies page on Inside NSF. General standards of employee conduct remain in effect as outlined in Standards of Ethical Conduct. Employees unclear about these policies and standards should discuss them with their supervisor or consult with the Office of General Counsel (OGC).
- Know and comply with NSF's Standard Operating Procedure (SOP) for General Social Media. This document specifies privacy, comment, and image use policies, along with the procedures for starting a NSF social media account. The SOP is available on Inside NSF.
- Know and comply with NSF policy on protecting the privacy of sensitive information. Employees should not post information about program announcements that have not yet been cleared; pending or unfunded proposals; merit reviews; pre-decisional budget information, personally identifiable information; or other sensitive data.
- Respect copyright and financial disclosure laws. Exercise vigilance when posting ideas, concepts, or content to which an individual might claim ownership; rightful attribution is a keystone of responsible use of social media. Employees must secure explicit permission from the owner/creator of an image or video prior to posting.
- The laws, regulations, and policies that govern Federal records management (including the creation, maintenance/use, and disposition of records) also apply when creating social media on behalf of NSF. New content created with social media tools that qualifies as a federal record must be captured and maintained consistent with NSF Records Management policies. Contact the NSF Records Officer with questions about capturing social media records. See NSF Records Retention Schedule.

4.2. Personal use of social media when an individual identifies as an NSF employee

- When employees are on duty, they must use official time in an honest effort to perform official duties. This limits the extent to which employees may access and use their personal social media accounts while at work. A supervisor may not order or ask a subordinate to work on the supervisor's personal social media account.
- An employee may identify his or her official NSF title or position in an area of the personal social media account designated for biographical information. According to the U.S. Office of Government Ethics (OGE) Standards of Conduct, employees are prohibited from using their official titles, positions or any authority associated with their public offices for private gain. To evaluate whether a reference to an official title or position on social media violates the Standards of Conduct, see the relevant factors listed in Section 2 of the OGE Legal Advisory (LA-15-03).
- Use a disclaimer. When employees publish to a social media platform, they must be clear that what they say there represents their views and opinions, not the views and opinions of NSF. A disclaimer may state something like: "The postings on this site are my own and do not necessarily represent my employer's positions, strategies, or opinions."
- Employees seeking or negotiating for employment through social media must comply with the provisions set out in Subpart F of the Standards of Conduct and with Section 4 of the OGE LA-15-03 on the Standards of Conduct as Applied to Personal Social Media Use.
- Employees may use personal social media accounts to fundraise for nonprofit charitable organizations in a personal capacity, but they must comply with 5 C.F.R. § 2635.808, the section

of the Standards of Conduct that covers fundraising. As a general rule, fundraising solicitations over social media are permissible so long as the employee does not "personally solicit" funds from a subordinate or a known prohibited source. An employee may not respond to inquiries posted by prohibited sources or subordinates in reference to the fundraising request. Furthermore, an employee may not specifically reference, link to, or otherwise target a subordinate or known prohibited source when fundraising over social media. Additionally, employees may not use their official titles, positions, or authority associated with their positions to further fundraising efforts. See Section 6 of the OGE LA-15-03.

- Employees may not disclose nonpublic information to further their private interests, or the interests of others. Employees must follow the rules regarding the disclosure of nonpublic information found in the Standards of Conduct and all other applicable rules when using social media. The Standards of Conduct generally do not prevent employees from discussing or sharing government information that is publicly available. Employees may not, however, accept compensation for statements or communications made over social media that relate to their official duties. See Section 5 of the OGE LA-15-03.

4.3. General Social Media Best Practices

While NSF does not govern the use of social media beyond the scope of its workers' employment, employees are encouraged to consider these best practices for general use.

- When using social media, employees should always be cognizant of their NSF responsibilities. By virtue of their positions, they must consider whether personal thoughts published, even in clearly personal venues, may be misunderstood as expressing official NSF positions. Employees should assume anyone can read what they write, including colleagues.
- Employees should be aware of their NSF association in online social networks. If an employee identifies him/herself as an NSF employee or has a position for which his/her NSF association is known to the public, it is important to ensure that profile(s) and all related content (even if they are of a personal nature) are (a) consistent with how he/she wishes to present him/herself as an NSF professional; (b) appropriate with the public trust associated with the position; and (c) in conformance with existing standards such as NSF's standards of ethical conduct.
- Even if employees do not identify themselves as NSF employees in social media, the use of a disclaimer is strongly recommended. When employees publish to a social media platform, they should be clear that what they say there represents their views and opinions, not the views and opinions of NSF. A disclaimer may state something like: "The postings on this site are my own and do not necessarily represent my employer's positions, strategies, or opinions."
- Be mindful that social media content is widely accessible and persistent in the public domain. Exercise good judgment and consider content carefully before publishing.
- Employees should consider carefully when to use an NSF email address to register accounts. If the purpose is primarily social, use a personal email address.
- Employees should understand what they are signing up for. When using a social media site for the first time, read the Terms of Service carefully to be certain of understanding, and being capable of adhering to, the rules governing a site's use.
- Respect copyright and financial disclosure laws. Exercise vigilance when posting ideas, concepts, or content to which an individual might claim ownership; rightful attribution is a keystone of responsible use of social media. 4

- Exercise caution when accessing social media sites or downloading social media applications on NSF-provided mobile devices. Be sure to follow best practices for social media security, such as downloading social media applications only through reputable sources and reading applications privacy and security policies before adding them onto a device.

5. Enforcement

Violation of this policy could result in disciplinary action up to and including removal and/or civil or criminal penalties, including personal financial liability for the cost of improper use.

APPENDIX E NSF IT SECURITY AND PRIVACY AWARENESS TRAINING RULES OF BEHAVIOR

This section presents the NSF IT Security and Privacy Awareness Training Rules of Behavior, as published in NSF Annual Security Awareness Training.

These Rules of Behavior detail the responsibilities of and expectations for all NSF employees and contractors that use NSF IT resources (i.e., IT systems and information). The Rules of Behavior supplement existing NSF policy by enhancing and further defining the specific rules each user must follow while accessing NSF IT resources. As a user of NSF IT resources, I acknowledge and will comply with the following:

Appropriate Use

- I may be provided with electronic tools such as computers, cell phones, and personal electronic devices to accomplish my official duties. I will use only the systems, software, and data which I am authorized to use.
- I understand that I am responsible for proper use of all IT resources, and for any misuse of such IT resources. I understand that personal use is authorized in accordance with NSF policy.
- I understand that NSF monitors the use, storage, and transmission of information, and that there is no right to privacy for any aspect of my use of NSF electronic resources, including but not limited to any information I may transmit or store on a NSF system.
- I will not seek, transmit, collect, or store defamatory, discriminatory, harassing, or intimidating material that could discredit NSF or damage its public reputation.
- I will not seek, transmit, collect, or store obscene, pornographic, or sexually inappropriate material.
- I will follow all NSF policies for passwords, virus protection, prevention and reporting of security issues.
- I understand that the use of Peer to Peer software is prohibited per NSF policy.
- I understand that my use of social media must be conducted in line with the NSF Social Media Policy and government best practices.

Protection of Information

- I understand that I am responsible for recognizing and safeguarding all sensitive information in my control, including personally identifiable information (PII) such as Social Security Numbers. I will prevent inappropriate access, use, or disclosure of sensitive NSF information in all formats, whether onsite at NSF or at a remote location. (Note: “Personally identifiable information” refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc.)
- I will ensure appropriate protections when storing, transporting, transferring, e-mailing, remotely accessing, or downloading sensitive information, including PII, per NSF policy. I will ensure proper disposal of sensitive information when its use is no longer required.
- I will ensure compliance with NSF policy for the encryption of sensitive data.

Individual Accountability

- I understand that failure to comply with the Rules of Behavior or other requirements of NSF policy may result in disciplinary action, sanctions, personal liability, or criminal penalties.
- I read and fully understand the IT Security and Privacy Awareness training.
- I will complete required actions associated with the NSF Onboarding and Separation Policy.

END