THE NATIONAL SCIENCE FOUNDATION

Office of Polar Programs

**United States Antarctic Program**

**AIL-POL-5000.06**

**Acceptable Use of USAP Information Resources**

Effective Date: February 2023

Review Date: February 2028

Short, Stephanie A. Digitally signed by Short, Stephanie A. Date: 2023.03.09 15:44:30 -05'00'

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

## 1.0 Purpose

This policy 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 policy defines acceptable and prohibited personal use of USAP technology and communication resources.

## 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 USAP Rules of Behavior (RoB) for USAP participants to follow at all times. These are provided in Appendix A to this policy. Additional USAP applications may have Rules of Behavior specific to that application.

## 4.4 Controlled Unclassified Information (CUI)

Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended. (National Archives)

## 4.5 Non-public NSF Information or Data

Non-public information is information that is gained through employment at NSF, including employment as a contractor, that has not been made available to the general public. Ethics regulations (5 C.F.R. § 2635.703(b)) define non-public information as:

> *…information that the employee gains by reason of Federal employment and that he knows or reasonably should know has not been made available to the general public. It includes information that he knows or reasonably should know:*

> *(1) Is routinely exempt from disclosure under 5 U.S.C. § 5523 or otherwise protected from disclosure by statute, Executive order, or regulation;*
> *(2) Is designated as confidential by an agency; or*
> *(3) Has not actually been disseminated to the general public and is not authorized to be made available to the public on request.*

Examples of NSF or USAP non-public information include:

- Information from or about pending proposals;
- Information from or about pending awards;
- Information from or about declined proposals, at any stage;
- Information from or about pending solicitations;
- Pre-decisional NSF budget information;
- Program success rates;
- Reviewer identities;
- PI and reviewer demographic information.

## 4.6 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.

## 4.7 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.

## 4.8 Personally Identifiable Information (PII)

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)

The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important to recognize that non-PII can become PII whenever additional information that is publicly available — in any medium and from any source — is or can be combined to identify an individual. As an example, PII includes a name or an email address because these pieces of information uniquely identify an individual, but alone may not constitute Sensitive PII.

## 4.9 Sensitive PII

Sensitive PII refers to information that can be used to target, harm, or coerce an individual or entity, assume or alter an individual's or entity's identity, or alter the outcome of an individual's or entity's activities. Sensitive PII requires stricter handling because of the increased risk to an individual if the information is compromised. Some categories of Sensitive PII include stand-alone information, such as biometric identifiers. Other information such as a financial account, date of birth, maiden names, citizenship status, or medical information, in conjunction with the identity of an individual (directly or indirectly inferred), are also considered Sensitive PII. The context of the information may determine whether it is sensitive, such as a list of employees with poor performance ratings or a list of employees who have filed a grievance or compliant.

## 4.10 Protected Health Information (PHI)

Individually identifiable health information that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. Protected Health Information is a component of Personally Identifiable Information (PII).

## 4.11 Sensitive Information

Sensitive Information is any information, which if lost, compromised, or disclosed, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual, the Government, or the Government's interests. Sensitive Information is subject to stricter handling requirements because of the increased risk if the data are compromised. Some categories of sensitive information include financial, medical or health, legal, strategic, proprietary, and human resources. These categories of information require appropriate protection as stand-alone information and may require additional protection in aggregate.

Basic types of Sensitive Information 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
- USAP IT infrastructure information
- Detailed internal USAP network diagrams
- USAP Information Technology information
- Root or system administrator passwords to systems on the USAP network

- USAP Vulnerability scan results
- USAP System log files

## 4.12 Social Media

A general term that is defined as forms of electronic communication through which users create online communities to share information, ideas, personal messages, and other content (such as videos). Social media tools include, but are not limited to, technologies such as blogs (e.g., WordPress), wikis (e.g., Wikipedia), social networks (e.g., LinkedIn, Facebook, Twitter, Instagram), and digital boards (e.g., Pinterest).

## 4.13 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:

- Government Owned Contractor Operated (GOCO) Systems - U.S. Government owned systems where a contractor provides design, development, deployment, operations, and/or phase-out.
- 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:
- 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.
- Contractor Owned – Interconnected (CO-Int) Systems - All contractor owned systems that are directly connected with USAP information systems (including USAP networks).

## 4.14 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:

- 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.
- 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.
- 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.

# 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*. and incorporated here in Section 5.1.

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 21-16, *Policy for Social Media Use*, and is included in Appendix B 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 NSF USAP Rules of Behavior (Appendix A) which include the USAP Sensitive Rules of Behavior. 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 NSF USAP 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 Rules of Behavior prior to accessing sensitive information and annually thereafter.

## 5.1 Personal Use Policy for NSF USAP Technology and Communication Resources

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 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

## 5.2 USAP Rules of Behavior

All USAP participants and any other person who uses USAP information systems or otherwise accesses USAP information must review and acknowledge the NSF USAP Rules of Behavior before being granted access, and at least annually thereafter while they have access to the USAP information systems.

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

OPP may establish Rules of Behavior for specific USAP information systems and applications as needed.

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.

## 5.3 Social Media Use

All users of USAP information systems must adhere to NSF OD 21-16, *Policy for Social Media Use* (Appendix B) when using social media in their USAP activities.

The NSF *Policy for Social Media Use* 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 you create, contribute to, or participate in social media on behalf of NSF or the USAP, you are expected to follow all NSF directives for social media use.

You must distinguish personal social media pages from official NSF or USAP social media accounts.

Be aware of your NSF and USAP association in online social networks.

Protect Sensitive Information - Do not post information about program announcements that have not yet been cleared, pending or unfunded proposals, merit reviews, personally identifiable information, or other sensitive data.

Respect Laws – Follow copyright, fair use, and financial disclosure laws. See Policy for Social Media Use before using images and videos from the Internet in NSF documents.

Be mindful - Be cognizant of NSF responsibilities. Consider whether personal thoughts published, even in clearly personal venues, may be misunderstood as expressing official NSF positions. Assume anyone can read what is written, including colleagues. It is always advisable to include a disclaimer.

If accessing social media for personal purposes while at work, employees must comply with the NSF and USAP policies, to include this policy and the Rules of Behavior.

## 5.4 No Expectation of Privacy

OPP does not 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 because of unauthorized activity by participants or by others outside the program.

## 5.5 Acceptable Uses of USAP Information Resources

The following activities are considered acceptable uses of the USAP GSS. 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.

## 5.6 Prohibited Uses of USAP Information Resources

The following activities are prohibited uses of the USAP GSS or its components.

All illegal activities are forbidden.

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 Technology.** 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.

## 5.7 Additional Guidance for Users

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 this policy and the 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 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 because 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 Enterprise Service Desk at 720-568-2001 or ITCEnterpriseServiceDesk@usap.gov. Additional information may be found at www.usap.gov.

## 5.8 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.** As part 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.

## 5.9 USAP Sensitive Information

**User Responsibilities.** While performing official duties, USAP participants with access to Sensitive Information (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.

**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 NSF policy, users must immediately report actual and potential incidents of inappropriate disclosure of SI or PII to the USAP Enterprise Service 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.

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 Roles and Responsibilities

See AIL-POL-5000.01, *USAP Information Security and Privacy Program*.

## 7.0 Compliance

Failure to comply with information security and privacy policies may result in revocation of access to USAP information technology resources and may also result in disciplinary action.

## 8.0 Policy Management and Review

See AIL-POL-5000.01, *USAP Information Security and Privacy Program*.

## 9.0 Management Commitment

See AIL-POL-5000.01, *USAP Information Security and Privacy Program*.

## 10.0 Coordination Among Organizational Entities

See AIL-POL-5000.01, *USAP Information Security and Privacy Program*.

## 11.0 References

See AIL-POL-5000.01, *USAP Information Security and Privacy Program*.

**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 |
| 5.0 | 6/17/2022 | Update for NIST SP 800-53, Revision 5 | NSF/OPP |
| 5.1 | 11/16/2022 | Reviewed and updated as needed in all sections | NSF/OPP |
| 5.2 | 2/24/2023 | Final for signature and publication | NSF/OPP |

# APPENDIX A NSF USAP RULES OF BEHAVIOR

This Appendix contains the NSF USAP Rules of Behavior for Access to USAP IT Resources Including Sensitive Information, Non-public and Personally Identifiable Information (PII).

The National Science Foundation (NSF) Office of Polar Programs (OPP) manages the U.S. Antarctic Program (USAP) to support scientific research in Antarctica and the Southern Ocean, to include the USAP information systems. The Rules of Behavior detail the responsibilities and expectations for all USAP participants that use USAP information systems and information. This includes, but is not limited to, the following: NSF and other federal agency employees and contractors, military personnel, science grant team members, and visitors. The Rules supplement existing NSF and USAP policy by defining the rules each user must follow while accessing USAP IT resources.

---

**Rules of Behavior for Access to USAP IT Resources**

As a user of NSF USAP IT resources, I acknowledge I have reviewed USAP Information Security and Privacy Literacy/Awareness Training, or the equivalent training provided by my federal agency, and I will comply with the following rules:

*Appropriate Use*

- I may be provided with electronic tools and/or access to USAP networks, computers, mobile devices, and personal electronic devices to accomplish my official duties.
- I will use only the systems, software, and data for which I have authorization and use them only for official government business or in accordance with NSF and OPP USAP policies and procedures.
- I understand that NSF monitors the use, storage, and transmission of information, and I have no right to privacy for any aspect of my use of USAP electronic resources, including but not limited to any information I may transmit or store on a USAP system.
- I will not seek, transmit, collect, or store defamatory, discriminatory, harassing, or intimidating material that could discredit NSF or the USAP or damage NSF's public reputation.
- I will not seek, transmit, collect, or store obscene, pornographic, or sexually inappropriate material.
- I will follow all NSF and USAP policies for passwords, virus protection, prevention, and reporting of security issues.
- I understand that my use of social media must be conducted in a manner consistent with the NSF Social Media Policy, USAP policy, and government best practices.
- I understand that I must avoid using my USAP email address as an identifier for any non-NSF online service, system, or account.

*Individual Accountability*

- I understand that failure to comply with the Rules of Behavior or other requirements of NSF or USAP policies may result in disciplinary action, sanctions, personal liability, or criminal penalties.
- I have completed all required Information Security training and acknowledgements.
- If applicable, I will complete required actions associated with the NSF Onboarding and Separation Policy.

**Rules for Access to Sensitive, Non-public and Personally Identifiable Information (PII)**

The rules detail the responsibilities and expectations for all individuals with access to sensitive information. The term "sensitive information" includes business sensitive information, non-public, Personally Identifiable Information (PII), and Protected Health Information (PHI).

*Responsibility and Accountability*

- I understand that I am responsible for recognizing and safeguarding all business sensitive, non-public, PII and PHI in my control, including but not limited to Social Security Numbers (SSN).
- I will prevent inappropriate access, use, or disclosure of business sensitive USAP information in all formats, whether at a USAP operating location, at a remote location, or at an alternate work site.
- I understand that with access to systems and data that use PII or PHI, especially those with access to SSNs, I must view and access this information only for the intended purposes for which the data were collected.

*Storage and Transmission*

- I will store all records containing business sensitive information on secure USAP services or devices, e.g., USAP SharePoint, with access limited to those individuals or entities that require access to perform a legitimate NSF or USAP job function within their official duties.
- I will ensure compliance with NSF and USAP policy for the encryption of sensitive and PII/PHI data. I will not store business sensitive information on portable devices such as laptops, mobile devices, and USB drives unless encryption is employed.
- I understand all removable or transportable media (e.g., paper-based documents, reports, CDs, USB drives, etc.) containing business sensitive information must be properly secured. Reasonable security measures depend on the circumstances, and may include locked file rooms, desks, cabinets, and encryption.
- I will not transmit SSNs through USAP email, chat tools, or other online collaboration tools. This includes the last four or five digits of SSNs.

*Disposition*

- I understand that subject to applicable document retention policies or unless required by law, paper documents and electronic media containing sensitive information that is no longer needed must be destroyed or disposed of using methods designed to prevent subsequent use or recovery of information.

*Reporting*

- I understand I must report security and/or privacy-related incidents and any incidents of suspected fraud, waste, or misuse of USAP systems to appropriate officials.

**I understand that failure to comply with the Rules of Behavior or other requirements of NSF or USAP policy may result in disciplinary action, sanctions, personal liability, and/or civil or criminal penalties.**

**I acknowledge receipt of, understand my responsibilities, and will comply with the NSF USAP Rules of Behavior stated above.**

**Overview of Information Types**

The term, Information, is synonymous with Data, regardless of format or medium. Sensitive information is the overarching category that includes non-public information and Personally Identifiable Information (PII) and sensitive PII such as Protected Health Information (PHI).

**1. Sensitive Information:** Sensitive Information is any information, which if lost, compromised, or disclosed, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual, the Government, or the Government's interests. Sensitive Information is subject to stricter handling requirements because of the increased risk if the data are compromised. Some categories of sensitive information include financial, medical or health, legal, strategic, proprietary, and human resources. These categories of information require appropriate protection as stand-alone information and may require additional protection in aggregate.

**2. Personally Identifiable Information (PII):** PII, as defined in OMB Memorandum M-07-16 *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, refers to information that can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important to recognize that non-PII can become PII whenever additional information that is publicly available — in any medium and from any source — is or can be combined to identify an individual. As an example, PII includes a name or an email address because these pieces of information uniquely identify an individual, but alone may not constitute Sensitive PII.

**3. Sensitive PII:** Sensitive PII refers to information that can be used to target, harm, or coerce an individual or entity, assume or alter an individual's or entity's identity, or alter the outcome of an individual's or entity's activities. Sensitive PII requires stricter handling because of the increased risk to an individual if the information is compromised. Some categories of Sensitive PII include stand-alone information, such as biometric identifiers. Other information such as a financial account, date of birth, maiden names, citizenship status, or medical information, in conjunction with the identity of an individual (directly or indirectly inferred), are also considered Sensitive PII. The context of the information may determine whether it is sensitive, such as a list of employees with poor performance ratings or a list of employees who have filed a grievance or compliant.

**4. Non-public NSF information or data:** NSF Staff Memorandum OD 18-10 *Sharing of Non-public NSF Information – Interim Guidance*, provides direction on the protection and use of non-public information. Non-public information is information that is gained through employment at NSF, including employment as a contractor, that has not been made available to the general public. Ethics regulations (5 C.F.R. § 2635.703(b)) define non-public information as:

> *…information that the employee gains by reason of Federal employment and that he knows or reasonably should know has not been made available to the general public. It includes information that he knows or reasonably should know:*
>
> *(1) Is routinely exempt from disclosure under 5 U.S.C. § 5523 or otherwise protected from disclosure by statute, Executive order, or regulation;*
>
> *(2) Is designated as confidential by an agency; or*

*(3) Has not actually been disseminated to the general public and is not authorized to be made available to the public on request.*

Examples of non-public information include:

- Information from or about pending proposals
- Information from or about pending awards
- Information from or about declined proposals, at any stage
- Information from or about pending solicitations
- Pre-decisional NSF budget information
- Program success rates
- Reviewer identities
- Personnel information such as information about candidates who come to NSF to give talks for an open position
- PI and reviewer demographic information.

**5. Controlled Unclassified Information (CUI):** Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended. (National Archives definition)

**6. Protected Health Information (PHI):** Individually identifiable health information that is: (i) Transmitted by electronic media; (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium. Protected Health Information is a component of Personally Identifiable Information (PII).

END of Appendix A

# APPENDIX B 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 21-16, *Policy for Social Medial Use*. Where applicable, information specific to USAP participants is noted here.

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 21-16, *Policy for Social Medial Use*. For this policy, the term “staff” includes all USAP participants.

## 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 "staff." This policy also applies to others who have access to NSF equipment, computing services, or communication systems.

## 2. Definition

"Social media" is a general term that is defined as forms of electronic communication through which users create online communities to share information, ideas, personal messages, and other content (such as videos). Social media tools include, but are not limited to, technologies such as blogs (e.g., WordPress),wikis (e.g., Wikipedia), social networks (e.g., LinkedIn, Facebook, Twitter, Instagram), and digital boards(e.g., Pinterest).

## 3. Purpose

This document establishes policy for the use of social media by NSF staff while working for NSF. This policy will evolve as new technologies and social media tools become available. Social media creates new opportunities for engagement and new vulnerabilities. Therefore, NSF staff who use social media are required to do so 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.

## 4. Policy

The Office of Legislative and Public Affairs (OLPA) has the authority and is responsible for communicating to external audiences’ information about the activities, programs, research results, and policies of NSF. In addition, OLPA oversees all NSF-branded social media accounts and manages the agency’s online presence on sites like Facebook, Instagram, LinkedIn, Twitter, Pinterest, and YouTube.

Individual directorate or division-level social media accounts or online groups (on sites like LinkedIn) representing NSF or NSF programs are not permitted. Accounts discovered operating outside of OLPA management will be in violation of this policy and result in closure of the Individual directorate or division-level social media accounts or online groups (on sites like LinkedIn) representing NSF or NSF programs are not permitted. Accounts discovered operating outside of OLPA management will be in violation of this policy and result in closure of the social account. Instead, NSF staff should contribute content ideas for posting consideration on NSF’s official social media sites. OLPA welcomes staff to share their ideas with their communication liaison or directly with the social media team at socialmedia@nsf.gov.

Staff who contribute to NSF's social media presence should review, understand, and comply with all relevant agency policies and directives outlined in Sections 4.1 and 4.2. The social media best practices described in Section 4.3 are provided as guidance only.

## 4.1 Social Media Use in Official Capacity

Staff who create, contribute to, or participate in social media on NSF behalf are expected to exercise decorum and professionalism and to comply with all relevant agency policies and directives including:

- 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 InsideNSF. 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 the General Counsel (OGC).
- NSF's Standard Operating Procedure (SOP) for Social Media. This document specifies privacy, comment, and image use policies. The SOP is available on InsideNSF.
- NSF's Logo and Visual Identity Guidelines. This document specifies use of logos, visual elements, and co-branding. The guidelines are available on NSF.gov.
- NSF policy on protecting the privacy of sensitive information. Staff 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.
- Copyright and financial disclosure laws. Exercise vigilance when developing ideas, concepts, or content to which an individual might claim ownership; rightful attribution is a keystone of responsible use of social media. Staff 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 Records Management staff with questions about capturing social media records. See NSF Records Retention Schedule.

## 4.2 Personal use of social media as an NSF employee

NSF staff should be aware of their NSF association in online social networks. If staff members identify themselves as NSF employees or have a position for which their NSF association is known to the public, it is important to ensure that profile(s) and NSF-related content (even if they are of a personal nature) are:

- consistent with how he/she wishes to present themselves as an NSF professional;
- appropriate with the public trust associated with the position; and
- in conformance with existing standards such as NSF's standards of ethical conduct.

Staff may identify their official NSF title or position in an area of the personal social media account designated for biographical information. However, according to the U.S. Office of Government Ethics (OGE) Standards of Conduct, staff are prohibited from using their official t 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).

Whether staff identify their NSF position on social media or not, they 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. Staff should assume anyone can read what they write, including colleagues. Staff is encouraged to identify their posts as their own personal views. See section 4.3 for general guidance on recommended disclaimer language.

**Personal Social Use on Official Time**

When on duty, staff 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. 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.

Staff may not disclose nonpublic information to further their private interests, or the interests of others. NSF staff 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. Staff 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.

**Seeking Employment on Social Media**

Agency staff 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.

**Fundraising on Personal Social Accounts**

NSF staff may use personal social media accounts to fundraise for nonprofit charitable nonpolitical 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.

## 4.3 General Social Media Best Practices

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

- Agency staff are permitted to follow NSF’s official social media accounts and share content from NSF’s accounts with their personal networks. Sharing publicly available content from the agency’s social sites protects staff from inadvertently disclosing non- public information.
- Even if NSF staff do not identify their NSF position on social media – it is strongly recommended that they clarify that their posts represent their personal 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 NSF's positions, strategies, or opinions."

- 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.
- Staff should be mindful that social media content is widely accessible and persistent in the public domain. Exercise good judgment and consider content carefully before publishing.
- 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.
- The Hatch Act limits the extent to which executive branch employees may use social media to engage in certain political activities. See U.S. Office of Special Counsel, Frequently Asked Questions Regarding the Hatch Act and social media.

## 5. Enforcement

Violation of this policy could result in disciplinary action up to and including removal from federal service.

END