NSF Rules of Behavior for Access to IT Resources
Including Sensitive Information, Non-public and Personally Identifiable Information (PII)

The Rules of Behavior detail the responsibilities and expectations for all NSF staff (employees, IPAs, contractors and all other personnel) that use NSF IT systems and information. The Rules supplement existing NSF policy by defining the rules each user must follow while accessing NSF IT resources.

Rules of Behavior for Access to IT Resources

As a user of NSF IT resources, I acknowledge I have reviewed NSF IT Security and Privacy Awareness Training and will comply with the following rules:

Appropriate Use

- I may be provided with electronic tools such as 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 the Personal Use Policy for NSF's Technology and Communication Resources.
- 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 NSF electronic resources, including but not limited to any information I may transmit or store on an 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 my use of social media must be conducted in a manner consistent with the NSF Social Media Policy and government best practices.
- I understand that I must avoid using my NSF 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 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.

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, and Personally Identifiable Information (PII).

Responsibility and Accountability

- I understand that I am responsible for recognizing and safeguarding all business sensitive, non-public, and Personally Identifiable Information (PII) in my control, including but not limited to Social Security Numbers (SSN).

- I will prevent inappropriate access, use, or disclosure of business sensitive NSF information in all formats, whether onsite at NSF or at a remote location.
- I understand that with access to systems and data that use PII, 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 NSF services, e.g., One Drive, SharePoint, with access limited to those individuals or entities that require access to perform a legitimate Foundation job function.
- I will ensure compliance with NSF policy for the encryption of sensitive and PII 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 forms, reports, CDs, USB drives, etc.) containing business sensitive information must be properly secured. Reasonable security measures depend on the circumstances, but may include locked file rooms, desks, cabinets, and encryption.
- I will not transmit SSNs through NSF email, Skype for Business 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 NSF systems to appropriate officials.

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, and/or civil or criminal penalties.

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

_____ _____ _____

Signature NSF Division/Company Date of Signature

Printed Name _____

For IT Help Central Use:

_____ _____ _____

Ticket Number IT Help Central (Printed Name) Date Received

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 SSNs.

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 Social Security numbers (SSN) or 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 that has not been made available to the general public. Ethics regulations (5 C.F.R. § 2635.703(b)) define non-public information as:
    i. …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:
    ii. (1) Is routinely exempt from disclosure under 5 U.S.C. § 5523 or otherwise protected from disclosure by statute, Executive order or regulation;
    iii. (2) Is designated as confidential by an agency; or

iv. (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)