Information Security and Privacy Awareness / Rules of Behavior

Purpose

SSA is vital to the economic security of the United States. All SSA employees, who have been granted access to SSA information systems, hereafter referred to as "Authorized User(s)," are responsible for protecting information and information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information, hereafter referred to as "information system(s)" in the performance of their duties in support of SSA's mission.

Information security and privacy awareness training, as well as rules of behavior, are required of all Executive Branch government agencies and departments by the Office of Management and Budget (OMB) Circular A-130. Failure to follow prescribed rules or misuse of information and information systems, can lead to suspension, termination, or other administrative or legal actions based on the seriousness of the violation.

This document provides general information security and privacy awareness training and conveys SSA's information security and privacy awareness policy and security requirements, expectations, roles, and responsibilities.

Information Security

Information security is the protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

- **Confidentiality** preserves authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. It ensures that only authorized personnel access sensitive information and prevents unauthorized disclosure. To carry out the principle of confidentiality:
  - Only disclose information obtained while performing your work duties as legally authorized and consistent with the policy and procedures for that system;
  - Take precautions to prevent viewing by unauthorized individuals; and
  - Always promptly log-off or lock workstations when leaving devices unattended.
- **Integrity** guards against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. To carry out the principle of integrity:
  - Never intentionally enter unauthorized, inaccurate, or false information;
  - Review the quality of information as you collect, generate, and use it;
  - Never expose critical data or sensitive information to conditions that may compromise its integrity;
  - Protect agency furnished devices while on travel as well as at Alternate Duty Stations (ADS); and
  - Take appropriate training before using a system in order to minimize the potential for errors.
- **Availability** ensures timely and reliable access to information and resources by authorized personnel when needed. To carry out the principle of availability, ensure:
  - Effective security measures are in place to protect system components; and
  - Information is available for authorized users when they need to access it.

Safeguarding Sensitive Information

Sensitive Information is information protected from unauthorized disclosure. Sensitive information includes, but is not limited to, the following:

- **Personally Identifiable Information (PII)** - Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother`s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
- **Federal Taxpayer Information (FTI)** - Any return or return information received from the Internal Revenue Service or secondary source, and includes any information created by the recipient derived from the return or return information.
- **Protected Health Information (PHI)** - All individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.
- **Controlled Unclassified Information (CUI)** - Information the Government creates or possesses, or that an external entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

- **Payment Card Industry - Data Security Standard** - A set of standards that helps to protect cardholder data. It applies to all entities that store, process, or transmit cardholder or sensitive authentication information.
- **Proprietary Business Data** - Material and information relating to, or associated with, SSA products and services, business, or activities. These include, but are not limited to, SSA administrative data.

As an Authorized User, you must safeguard access to sensitive information and protect it against unwarranted disclosure, whether officially on duty or off duty, at your official duty station or another official work location or an ADS, and follow all agency guidance and policies regarding the protection of sensitive information.

Accountability

You are accountable for your activity when using SSA information systems. You must log on to the SSA network with your credential, also known as your Personal Identity Verification, or PIV credential. The agency authorizes access to information systems based on the information security principles of "Need-to-Know," and "Least Privilege." This ensures access is limited to authorized personnel who have a legitimate business need for these resources to perform their assigned position responsibilities.
Protect SSA information systems and sensitive information by:

- Complying with current information security, privacy, and confidentiality practices;
- Behaving in an ethically, informed, and trustworthy manner;
- Choosing passwords that comply with agency password policies;
- Being accountable for all transactions issued in connection with your PIV credential / Personal Identification Number;
- Never sharing your password with anyone;
- Obtaining formal authorization before accessing sensitive or critical applications;
- Using encryption to ensure that any sensitive information sent electronically is received by the correct entity and that it is not modified during transmission; and
- Only using your access for the performance of your official duties.

Hardware, Software, and Copyright Protection and Control

Configuration management standards are the first line of defense for the prevention of malicious activities on SSA networks.
Follow these rules when using SSA hardware and software:

- Only use SSA information systems and software purchased through the agency acquisition procedures or software that has been developed, evaluated, documented, or distributed in-house;
- Do not disable any SSA security features unless authorized by management;
- Use only approved SSA systems resources, connecting personally owned hardware, software, and media to SSA systems resources is prohibited;
- Take necessary precautions to protect SSA's equipment, laptops, and other Portable Electronic Devices against loss, theft, damage, abuse, or unauthorized use by employing appropriate protection measures;
- Protect copyright information in accordance with the conditions under which it is provided and Federal copyright laws;
- Do not make illegal copies of software;
- Follow agency policies on limited personal use of government furnished equipment, if applicable;
- Comply with all agency policies and procedures regarding the use of e-mail; and
- Properly safeguard removable media.

Secure Email and Fax Use

Use business communication tools in a responsible, secure, and lawful manner. There should be no expectation of privacy while using SSA information technology resources, including email and fax.
For those using SSA email, to protect agency systems and those who receive email from you:

- Do not send or forward any form of sensitive information, as defined above, to a non-SSA email address unless the information has been properly encrypted or the recipient is on the Agency's Secure Partners List;
- Do not send or forward any form of sensitive information, as defined above, using a non-SSA email account;
- Do not copy or blind copy work related email to a personal, non-SSA email address;
- Do not send or forward chain letters or other unauthorized mass mailings; and
- If you receive an email intended for someone else, immediately notify the sender and delete or destroy the misdirected message.

When using an SSA fax, to protect agency systems and those who receive faxes from you:

- Use a cover sheet marked "confidential" when faxing sensitive information;
- Do not leave fax machines unattended when transmitting or for reading by unauthorized individuals;
- Transmit faxes to the intended recipient. When possible, use pre-programmed fax numbers;
- Do not use SSA's fax system to create or distribute disruptive or offensive messages; and
- If you receive a fax by mistake, you should notify the sender. To the extent possible, do not read the fax's contents. Destroy the misdirected message.

Public Disclosure

Properly controlling the disclosure of information outside of the agency is critical to preserving the confidentiality, integrity, and availability of SSA information and information systems.

- Personnel must follow SSA's social media policies when using social media web sites for both official business and personal use;
- Ensure that appropriate SSA management officials approve the external release of agency records and information, including through public access channels for public dissemination. Consult with the Office of Communications and the Office of Privacy Disclosure, as appropriate, regarding approved methods for publicly disseminating agency records and information;
- Never transmit, store, or process sensitive information on external sites, unless explicitly authorized to do so. This includes social media, online forums, third-party collaboration tools or sites, social networking sites, and any other non-SSA-hosted sites, including unapproved third-party data storage providers; and
- Do not share programming code used for SSA information systems with unauthorized individuals. This includes, but is not limited to, posting code to unauthorized online forums, sending code to anyone not properly authorized to have it, or storing code on unapproved third-party sites.

Alternative Worksite (Non-SSA Controlled Locations)

Personnel eligible and approved to work at an Alternate Duty Station (ADS) must observe the following security guidelines:

- Follow the security and safety requirements of an alternative worksite agreement. If operating without such an agreement, ensure that SSA security and safety policies are applied;
- Adhere to agency information security policies and rules of behavior while at the ADS;
- Do not print any material that contains sensitive information at an individual's ADS; and
- Safeguard and properly dispose of any other sensitive information.

Social Engineering

Social engineering is tricking someone into divulging sensitive information or performing actions that may compromise the security of SSA. Common attack methods authorized users should be aware of and safeguard the agency and themselves against include:

- **Vishing** is the practice of tricking you, over the phone, into revealing sensitive information to an unauthorized individual; or performing actions on your workstation that may compromise the security of SSA.
  Avoid vishing attempts by validating a caller's identity and purpose. If you are unable to validate the caller's identity, hang up and call back using a number you know to be correct.
- **Phishing** is someone using social engineering techniques over email to trick you into revealing sensitive information, clicking on a malicious link, or opening a malicious attachment that can infect your workstation.
  - Avoid phishing attempts by verifying the email sender. Be suspicious when receiving emails from individuals you do not know or have not heard from in a long time. Never respond to requests for PII or send password information in an email. Only release information if you are confident of an individual's identity and right to receive it.
- **Social Data Mining** is someone using social engineering techniques to gather information about an individual or organization in public or social settings, including social media.
  - Avoid social data mining techniques by not sharing sensitive information to unauthorized individuals.
  - Be mindful of the information you post publicly on social media sites and, where possible, reduce the amount of information you make public.

Awareness and Training

Be alert to any indicators of system abuse or misuse. Complete mandatory information security and privacy awareness training within agency-defined timeframes. Participate in all required information security and privacy awareness and role-based training activities as identified by management, or as required by policy, agreement, or agency contract.

Incident Reporting

Incident reporting strengthens the agency through ongoing efforts to monitor, detect, and eliminate information security incidents. Timely incident reporting can help prevent the loss or theft of sensitive information and cyberattacks against the agency's network infrastructure.

- **Loss of Sensitive Information** - If you suspect or confirm the *loss or theft* of any sensitive information, including PII, you must report it within one hour to your supervisor, manager, contracting officer's representative-contracting officer's technical representative or another designated official. If those individuals are not available, please use the PII Loss Prevention Tool to report any loss of theft of any sensitive information or PII.
- **Malicious or Unauthorized Intrusion or Access** - if you observe a suspected systems intrusion attempt or other security-related incident, report the incident within 15 minutes of discovery to [redacted]@ssa.gov.
- **Phishing Attempt** - If you are the targeted victim of a *phishing* (suspicious email) attempt, report the incident within 15 minutes of discovery by clicking on the SSA Reporter button found on the Microsoft Outlook ribbon.
- **Vishing Attempt** - If you are the target of a *vishing* (suspicious phone call) attempt, report the incident within 15 minutes of discovery to [redacted]@ssa.gov.
- **Insider Threat** - If you observe a potential insider threat, an individual with authorized access attempting to wittingly or unwittingly harm the security of the agency through espionage, terrorism, unauthorized disclosure of sensitive information, or the loss or degradation of agency resources or capabilities, report the incident to [redacted]@ssa.gov.
- **Policy/Law Violation** - If you observe suspected violations of the Social Security Act, Privacy Act and other laws, as well as SSA policies and procedures, report the incident to the Office of the Inspector General (OIG) in accordance with published policy.

Prohibited Behavior

SSA has security guidelines prohibiting certain behaviors to help ensure the confidentiality, integrity, and availability of sensitive information. Prohibited behavior while using SSA information systems includes:

- Connecting personally owned hardware, software, or media to information systems;
- Using or copying SSA software in an unauthorized way;
- Altering agency devices, including all SSA supplied cell phones and mobile computing devices;
- Downloading unapproved software;
- Peer to Peer file sharing technology;
- Unauthorized web conferencing or "webinar" technology on agency networks;
- Accessing prohibited websites;
- Unauthorized modification or access to any device configuration;
- Unregistered modems;
- Unapproved forms of Instant Messaging solutions;
- Unauthorized use of scanning tools and devices; and
- Establishing multiple network connections from a single device.

Unauthorized Access and Consequences of Rules Violation

Unauthorized access to SSA information or information systems is prohibited. The agency monitors all network and system activity and has the ability to trace violations or attempted violations to individual information system users. Unauthorized access includes, but is not limited to, accessing programmatic information about:

- Yourself;
- Your children;
- Other family members;
- Former co-workers;
- Acquaintances; and
- Friends.

SSA has a published set of uniform sanctions for information systems access violations. In those instances, where authorized users do not follow the information security policies and prescribed rules of behavior, there are penalties that may be enforceable under existing policy and regulations ranging from official written reprimands through suspension of system privileges, temporary suspension from duty, removal from current position, to termination of employment, and possibly criminal prosecution.

- Users who fail to adequately safeguard sensitive information or who violate agency policies for safeguarding sensitive information may be subject to disciplinary action, up to and including removal from service or other actions in accordance with applicable law and agency policy.
- Supervisors may also be subject to disciplinary action for their failure to take appropriate action upon discovering a breach, or their failure to take required steps to prevent a breach from occurring, including adequately instructing, training, and supervising personnel regarding their responsibilities for safeguarding sensitive information.

Information Security and Privacy Awareness / Rules of Behavior Certificate of Completion

SSA Employees - Please complete all of the information below. Signing of this form constitutes acknowledgement that you have read, understand, and agree to abide by SSA's Information Security and Privacy Awareness and Rules of Behavior.

First Name: [redacted]

Last Name: [redacted]

Day Phone: [redacted]

I understand this training is mandatory and I am required to complete as part of my official duties. I understand that I can be subject to disciplinary action for making a false statement if I inaccurately certify completion of this training.

Date Inform[redacted]es of Behavior completed:

Signature: [redacted] Date: 03/05/2025

If your name or completion dates are omitted or illegible, or if your signature is omitted, this form will not be processed.