# Security and Privacy Awareness Training
# Contractor / Affiliate Personnel Security Certification

**Purpose:**

This training document is to be signed by contractor, subcontractor, or affiliate personnel, and those acting on behalf of the Social Security Administration (SSA) who have been granted access to SSA information and information systems to certify that they have received and understand SSA Information Security and Privacy Awareness Training detailed below.

**Background:**

SSA is vital to the economic security of the United States. In the performance of their duties in support of SSA's mission, all contractors, subcontractors, affiliates, and those acting on behalf of SSA who have been granted access to SSA information systems, hereafter referred to as "Authorized Users(s)," are responsible for protecting such information and information systems (e.g., hardware, software/applications, federal information/data, network, people) throughout the entire information life cycle, including collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Federal information includes information created, collected, processed, maintained, disseminated, disclosed, or disposed of by or for the Federal Government, in any medium or form.

Security awareness training is required for Authorized Users, per Section 44 USC 3554 of the Federal Information Security Modernization Act of 2014 (FISMA). Failure to follow prescribed rules or misuse of federal information and information systems can lead to criminal penalties, including fines and imprisonment, and disciplinary actions according to the contract and/or agreement under which I am performing work for SSA.

I understand that SSA maintains a variety of sensitive information about the agency's operations and programs, which may be information pertaining to program (e.g., information about SSA's clients) or non-program (e.g., administrative and personnel records) matters. I understand that SSA may authorize me to have access to federal information and information systems and that my access to and use of such information and information systems must be in accordance with the provisions of the contract and/or agreement under which I am performing work for SSA.

I understand that the terms in the contract and/or agreement under which I am performing work for SSA take precedence over this document. I understand that any questions I may have concerning authorization(s) to access SSA information and information systems should be directed in accordance with the terms of the contract and/or agreement. I have read, understand, and agree to the following conditions:

**Insider Threat**

An insider threat is someone with authorized access who uses that access, intentionally or unintentionally, to harm the security of the Agency or the Nation. The individual with authorized access may attempt 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.

- If I observe a potential insider threat, **I will** report the incident to SSAITP@ssa.gov and, as appropriate, in accordance with the personally identifiable information and incident reporting requirements in the contract or agreement under which I am working.
- **I will** safeguard federal information and information systems from exploitation, compromise, espionage, terrorism, or other unauthorized use and disclosure.

**Malware, Remote Access, and Mobile Device Security**

Malware encompasses malicious software, programs, files, and/or code in the form of virus, ransomware, and spyware that cause damage to information systems and data. SSA defends against malware using antivirus programs, intrusion detection systems, and social engineering training among other methods. Routine software and security updates ensure SSA devices are up to date with the latest malware protection.

When I have been granted an SSA device to perform work for the agency, the following requirements apply:

- In order to ensure my SSA device receives the necessary software and security updates**, I will** remain connected to SSANet using the agency's Virtual Private Network throughout my workday**, I will** keep my workstation plugged in and powered on, and **I will** restart my workstation at least once a week and at the end of each workday, logging off from the CTRL+ALT+DELETE screen unless further guidance is issued.

- **I will not** store federal information on personally owned media devices or, connect non-SSA approved and issued personal Bluetooth devices to an SSA device.

- **I will not** alter SSA devices, disable security settings, or download or install unauthorized software onto SSA devices.

- **I will** follow the security and safety requirements of any alternative worksite agreement and all contract or agreements related to non-SSA worksites.

- **I will not** print any material that contains federal information at an unapproved location. **I will** protect SSA devices at all times, to include while on travel, at any alternative worksite, and any approved non-SSA worksite.

**Secure Browsing and Social Media**

Attackers use social data mining techniques to gather information about an individual or organization in public or social settings, including social media. SSA social media accounts are not official SSA websites, but rather the department's presence on third-party service providers' platforms, which means SSA has limited control over how each platform uses personal data provided by users.

- **I will not** transmit, store, or process federal information on non-SSA owned and operated sites, including social media, third party online forums, third-party collaboration tools or sites, social networking sites, any other non-SSA-hosted sites, or unapproved third-party data storage providers unless explicitly authorized to do so.

- **I will not** share programming code used for federal information systems with unauthorized individuals including but 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.

- **I will not** use federal information systems to browse or access information about myself, my children, other family members, co-workers or former co-workers, acquaintances, and/or friends.

**Secure Email and Fax Use**

Email is an official business communication tool and users must use it in a responsible, secure, and lawful manner. When using SSA email, to protect agency systems and those who receive email from me:

- **I will** use business communication tools including SSA email in a responsible, secure, and lawful manner.
- **I will not** send or forward Personally Identifiable Information (PII) to or from a non-SSA email address unless the information has been properly encrypted or the recipient is on the Agency's Secure Partners List.
- **I will not** copy or blind copy work-related email to a personal, non-SSA email address.
- **I will not** send or forward chain letters or other unauthorized mass mailings.
- **I will not** configure my SSA email account to automatically forward work-related email to an outside (non-SSA, non-secure) address.
- If I receive an email intended for someone else, **I will** immediately notify the sender and delete or destroy the misdirected message.

A fax is an official business communication tool and users must use it in a responsible, secure, and lawful manner. When using an SSA fax, to protect agency systems and those who receive faxes from me:

- **I will** use business communication tools including SSA fax in a responsible, secure, and lawful manner.
- **I will** use a cover sheet that notes the sensitivity of the material and follow all Controlled Unclassified Information (CUI) labeling requirements.
- **I will not** leave fax machines unattended when transmitting.
- **I will** transmit faxes to the intended recipient, when possible, using pre-programmed fax numbers.
- **I will not** use SSA's fax system to create or distribute disruptive or offensive messages.
- If I receive a fax by mistake, **I will** notify the sender. To the extent possible, **I will not** read the fax's contents. **I will** destroy the misdirected message.

**Security Incident Reporting**

Security incidents involve any attempted or actual authorized access, use, disclosure, modification, or destruction of information. Examples include malicious or unauthorized intrusion or access, virus attacks, phishing, vishing, supply chain threats, foreign intelligence threats, insider threats, and loss of PII.

- If I suspect or confirm the loss or theft of any sensitive information, including PII, **I will** report it within one hour to my supervisor, manager, contracting officer's representative and/or contracting officer's technical representative or another designated official. If those individuals are not available, **I will** use the PII Loss Reporting Tool to report any loss or theft of any sensitive information or PII.
- If I observe a suspected systems intrusion attempt or other security-related incident, **I will** report the incident within 15 minutes of discovery to SOC@ssa.gov.
- If I am the targeted victim of a phishing (suspicious email) attempt, **I will** report the incident within 15 minutes of discovery by clicking on the SSA Reporter button found on the Microsoft Outlook ribbon.
- If I am the target of a vishing (suspicious phone call) attempt, **I will** report the incident within 15 minutes of discovery to SOC@ssa.gov.
- If I observe a potential insider threat, **I will** report the incident to SSAITP@ssa.gov. If I observe suspected violations of the Social Security Act, Privacy Act and other laws, as well as SSA policies and procedures, **I will** report the incident to the Office of the Inspector General in accordance with published policy.

**Social Engineering**

Vishing is the practice of tricking you, over the phone, into revealing information to an unauthorized individual or performing actions on your workstation that may compromise the security of SSA.

- **I will** avoid vishing attempts by validating a caller's identity and purpose.
- If I am unable to validate the caller's identity, **I will** hang up and call back using a number I 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.

- **I will** avoid phishing attempts by verifying the email sender.
- **I will** be suspicious when receiving emails from individuals I do not know or have not heard from in a long time.
- **I will** never respond to requests for PII or send password information in an email.
- **I will** only release information if I am confident of an individual's identity and right to receive it.

**Unauthorized Access and Prohibited Behavior**

Unauthorized access to federal 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. Federal information system users do not have a right, nor should they have an expectation, of privacy while using any Government office equipment at any time, including accessing the Internet using E-mail.

- **I will not** inspect, access, or attempt to access any federal information that SSA has not expressly authorized me to access.
- **I will not** release or disclose any federal information to any unauthorized person, agency, or entity. **I understand** that unauthorized disclosure of federal information may lead to civil penalties and/or criminal prosecution under Federal law (e.g., The Privacy Act of 1974, 5 U.S.C. 552a; SSA's regulations at 20 C.F.R. Part 401; The Social Security Act, 42 U.S.C. 1306 (a); and 5 U.S.C. Section 552(i)). **I further understand** that additional privacy and disclosure protections may apply to certain types of SSA information including Federal Tax Information (i.e., earnings information), which may be subject to additional penalties under sections 6103, 7213, 7213A, and 7431 of the Internal Revenue Service (IRS) Code (Title 26 of the United States Code).
- **I will** follow all access, retention, and/or destruction requirements in the contract and/or agreement under which I am authorized to access federal information. **I understand** that such requirements may require me to cease access to, return, or destroy federal information upon completion of my work for SSA or termination of my contract and/or agreement that authorized my access to federal information.
- **I will not** take federal information off-site, unless expressly authorized to do so by contract and/or agreement or other written authorization from SSA. If SSA authorizes me to take federal information off-site, I agree to safeguard all such information in accordance with agency policy and standards and the requirements of the contract and/or agreement under which I am performing work so that no unauthorized person, agency, or entity can access federal information.
- **I will** keep confidential any third-party proprietary information that may be entrusted to me as part of the contract and/or agreement, including safeguarding such information from unauthorized access and not disclosing or releasing such information unless expressly authorized to do so.
- **I will** follow all requirements in the contract and/or agreement under which I am performing work for SSA, includingbut not limited to those governing confidential information or PII.
- **I will** only use my access to federal information and information systems for the performance of my official duties.

| Contractor Employee Name (Print/Type) | Date (MM/DD/YYYY) |
|---|---|
| Contractor Employee Signature (Sign) | |
| Contract Number | Company Name (Print/Type) |
| Company Point Of Contact (Print/Type) | Company Point of Contact Phone Number |

## Privacy Act
## Collection and Use of Personal Information

42 U.S.C. § 904(a); 20 C.F.R. § 401.90; 44 U.S.C. §§ 3541-3549; 41 C.F.R. Chapter 101; 5 U.S.C. § 552a(e)(9)-(10); and Executive Order 13488 of the Social Security Act, as amended, allow us to collect this information. Furnishing this information to the Social Security Administration (SSA) is voluntary. However, failing to provide this information may affect your ability to access Federal information and information systems, which is a condition of the contract under which you are performing work for SSA (SSA contract). Not providing this information also could prevent us from issuing you a PIV credential and/or authorizing you to access SSA's network, one or both of which may be conditions of your SSA contract. Failure to follow prescribed rules or misuse of SSA information and information systems could lead to removal from duty from your SSA contract.

We will use the information you provide to grant you access to Federal information and information systems. We may also share your information for the following purposes, called routine uses:

- To contractors and other Federal agencies, as necessary, for assisting SSA in the efficient administration of its programs. We disclose information under this routine use only in situations in which SSA may enter into a contractual or similar agreement with a third party to assist the accomplishing an agency function relating to this system of records; and

- To student volunteers, individuals working under a personal services contract, and other workers who individuals performing functions for SSA but technically do not having the status of Federal agency employees, when they are performing work for SSA, as authorized by law, and if they need access to personally identifiable information (PII) in SSA the records in order to perform their assigned agency functions.

In addition, we may share this information in accordance with the Privacy Act and other Federal laws. For example, where authorized, we may use and disclose this information in computer matching programs, in which our records are compared with other records to establish or verify a person's eligibility for Federal benefit programs and for repayment of incorrect or delinquent debts under these programs.

A list of additional routine uses is available in our Privacy Act System of Records Notice (SORN) 60-0361, entitled Identity Management System, as published in the Federal Register (FR) on November 3, 2006, at 71 FR 64751. Additional information, and a full listing of all our SORNs, is available on our website at www.ssa.gov/privacy.