Safeguarding Personally Identifiable Information (PII)

Safeguarding Personally Identifiable Information

The United States Department of Agriculture (USDA) has made a risk management decision to exclude Information Security Awareness (ISA) training for technical service providers (TSPs) who are applying for certification, or being certified through, the NRCS TSP Program. USDA has determined that TSP users do not have access to USDA systems, network, or sensitive data, and therefore do not require ISA training for their limited access to the TSP Program Registry platform or receiving training through AgLearn.

This fact sheet provides guidance to help TSPs safeguard Personally Identifiable Information (PII) in paper or electronic form during their everyday work activities with producers participating in USDA programs.

What is PII?

PII is ANY information that permits the identity of an individual to be directly or indirectly inferred, including any information which is linked or linkable to an individual. Some PII is not sensitive, such as information found on a business card or official email signature block. This type of information does not require special handling. There is also PII, which if lost, compromised, or inappropriately disclosed, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Examples include: Social Security Numbers (SSNs), financial account numbers, birth dates, and biometricidentifiers (e.g., fingerprints and facial images). Other data elements such as citizenship or immigration status, account passwords, and medical information, in conjunction with the identityof an individual, are also considered PII. The context of the PII should be considered to determine potential risk impacts. Note that even when an individual's name is not present it may still be PII if it can be used to identify or be linked to an individual. PII can also be created when information about an individual is made available, or combined with other information.

Requirements for Protecting PII

- PII information in USDA records, whether in hard copy or electronic format, is protected from disclosure by Federal, USDA, and National Institute of Standards and Technology (NIST) Special Publication 800-122 requirements.
- The Privacy Act of 1974 protects individuals' sensitive information. This is the primary legislation that protects PII today.
- The e-Government Act of 2002, as amended, provides requirements for protecting Federal information, including privacy information.
- Section 1619 of the Food, Conservation, and Energy Act of 2008 protects confidential information provided to USDA by its participants.
- The Office of Management and Budget (OMB) provides guidance to the agencies of the Executive Branch of the Federal Government on how to implement laws on protecting privacy information.
- Key OMB guidance regarding Federal agency responsibilities for maintaining records - about individuals and protecting PII includes Circular A-130 and Memorandum M-17-12.

USDA Directives Supporting the Privacy Act

USDA implements the Privacy Act through guidance in the "USDA Privacy Program," as contained in several Departmental Manuals (or DMs) and Memoranda.

The USDA Privacy Program affirms that the privacy of an individual is a personal and fundamental right that should be respected and protected. USDA's privacy policy is located at https://www.usda.gov/privacy.

Breach Notification

A breach includes the loss of control, compromise, unauthorized disclosure, acquisition, or access by someone who is not allowed access to that PII. OMB defines a breach as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where: a person other than an authorized user accesses or potentially accesses PII, or an authorized user accesses or potentially accesses PII for an other than authorized purpose.

Reporting a PII Incident

Please immediately report any suspected or confirmed PII incidents to the PII Hotline at (877) PII-2-YOU, or (877) 744-2968. The hotline is operational twenty-four hours a day, seven days aweek. You can also e-mail cyber.incidents@ocio.usda.gov or contact the ASOC Hotline at (866) 905-6890.

By signing this PII Fact Sheet, I acknowledge receipt of the Safeguarding Personally Identifiable Information (PII), and I understand that pursuant to my role as a TSP to a client participating in a USDA program, I may be authorized by my client to have access to PII information in USDA records. I understand my responsibilities, and will comply with these responsibilities to protect PII.

TSP Signature: Date:

TSP First & Last Name (Print):

TSP Number:

TSP Email Address (email address affiliated with your eAuth ID):

Resident State (two letter abbreviation):