Procedure for the Management and Protection of Personal Identifiable Information (PII)

Amendment II

2021

TABLE OF CONTENTS

Page

PROCEDURE FOR THE MANAGEMENT AND PROTECTION OF PERSONAL IDENTIFIABLE INFORMATION OF PARTICIPANTS, VENDORS, SERVICE PROVIDERS, AND COLLABORATORS-2020

AMENDMENT II- Explanatory Statement

To comply with the requirement of protecting and guarantee the confidentiality of the Personal Identifiable Information of the Participants, Vendors, Service Providers, and Collaborators of AMSI; the following Subsections are amended:

D. Custody and Management of Information - includes the process that will be followed to transfer the files and the personal and confidential information of the participants (page 9).

G. Non-compliance – specific disciplinary actions are removed and depending on the seriousness of the offense, the corresponding disciplinary action will be applied, as established in the Human Resources Regulations of AMSI, Inc., revised (page 12).

The amended information is in bold and in a different **color**.

The additional terms and conditions of the Procedure remain unchanged.

Purpose

The purpose of this procedure is to protect and guarantee the confidentiality, proper use, and management of the Personal Identifiable Information (PII) of the participants, vendors, service providers, and collaborators of Alianza Municipal de Servicios Integrados, Inc. (AMSI). Also, to protect this information from disclosure related to the collection, storage, and distribution of sensitive data; and the use and application of the social security number in federal employment and training programs.

This procedure applies to all manual or mechanized documents, files, information systems, or records that are created, processed, accessed, or kept at AMSI.

In addition, the steps to be followed by anyone involved in information management and the disciplinary or legal actions applicable in the event of misuse or inappropriate disclosure of the information will be presented.

A. Personal Identifiable Information (PII)

PII is information that can be used to distinguish or ascertain the identity of an individual when alone or in combination with other personal or identifying data. IPP is classified in two categories:

- Protected PII – Information whose disclosure could be harmful to the person, by association with his name and identity.

  Examples:

  - Social Security Number
  - Credit Card Numbers
  - Bank Account Numbers
  - Phone Numbers

- Age
- Date of Birth
- Marital Status
- Name of Spouse
- Educational History
- Biometric Identifiers
- Medical History
- Financial Information
- Computer or Electronic Account Passwords

- Non-Sensitive PII- Information whose disclosure alone is not harmful to the individual.

  Examples:

  - Name and Surname
  - Email Address
  - Business or Work Address or Phone Number
  - Educational Credentials
  - Gender
  - Race

  However, depending on the circumstances, a combination of these elements can be categorized as protected or sensitive PII.

B. Applicants or Participants

When requesting the social security number, the process to follow will to:

- Hand the applicant or participant a Key Pad, where the applicant or participant will write their social security number.
  - This information will be reflected in the mechanized system, indicating if it is already registered, or if the information will be updated.

- If the participant does not agree to disclose the social security number, self-management services will be offered (job offers, employment statistics, occupations in demand, among others).
- In addition, it will be explained that this information will be used to calculate the results of the performance indicators, accountability on federal programs, etc.
- The participant will receive the Profile form (AMSI-2018 P/026), used to keep a record of people receiving services at the Centers. If the participant does not agree with filling out the entire form, they must complete at least the following details: name and surname, address, telephone numbers, emails, and interests, among others. It will be explained that this information will be useful for the identification of future service offerings. This information will be recorded in a mechanized information system (Excel, Access, etc.).
- Once the social security number (SS) is entered into the Mechanized Information System, it creates an identification number for the participant. This is a unique number that accompanies the participant throughout their participation. This number has twelve (12) digits, where the first four digits are zero (Example: 0000XXXXXXXX); and appears in the PRIS under: "Participant Identification Number (WIOA)".
- This Unique Identifier number will be used by the areas to process all transactions related to the participant.
- The Job Development and Training Coordinator (Job Career Coach) will be responsible for certifying that the social security number belongs to the participant. This certification will be made on the AMSI-2018 P/136 Universal Application form. The coordinator will then deposit this document in a legal-size manila envelope and file it, on the back-left side of the file; together with any document that contains this information.

- **For security reasons, they will not be able to keep a copy of the social security card to include it in the participant's file.**

C. Vendors, Service Providers and Colaborators

The process to follow is:

- The staff or officials who work with vendors, service providers, and collaborators, will require them to show their social security card and photo identification and will verify that the number is the one listed in the file and that it belongs to them. For security reasons, staff members will not be able to keep a copy of the social security card to include it in the file.
- Once the Vendors and Service Providers' social security or employer social security number is entered in the Mechanized Information System, an identification number or Vendor ID is created.
- The file number and Vendor ID will be used by the Areas to process all transactions related to the Vendors and Service Providers.
- Collaborators will identify themselves with the number assigned to them at the time of appointment. This will be their file number.
- All documents that require the social security number will be put in an envelope, sealed, and filed in the main file.

D. Custody and Management of Information

- Any Personal Identifiable Information contained in the files, information systems, or records will be used for the sole purpose of carrying out the public service's operations. It will be the responsibility of AMSI collaborators to take the necessary measures to guarantee the protection and privacy of all PII and to avoid the unauthorized disclosure of such information. To accomplish this, the following measures will be taken:

- All information considered as PII, as well as any other sensitive information that is transmitted by email or stored on CD's, DVD's, Jump Drives (USB sticks), etc., must be encrypted as described in the "Federal Information Processing Standards (FIPS) 140-2", and in compliance with the "National Institute of Standards and Technology (NIST). You shall not send unencrypted emails containing PII to any entity. To process a document with sensitive information and share it via email, the process is as follows:

    - Prepare the document in Word, Power Point, Excel.
    - Then choose: File – Info- Protect Document-Encrypt with Password- then write down a password and click OK. Validate the password and click OK once more.
    - Click the Back arrow and return to the document. Click: File-Save as- then select the folder where you will save the document and write down a name for it.
    - Prepare the email, insert the document, and send it.
    - Prepare a second email informing the recipient of the password needed to open the document.

    Two separate emails are sent to keep the PII data in the strictest confidence. One email contains the information or document; and another the password to open the document.

- All PII obtained during the handling and offering of services will be stored in a physically secure area, with access limited to authorized personnel. The information will be processed using equipment, technology, and locations approved by the Employment and Training Administration (ETA). The access, processing, and storage of PII obtained for the handling and offering of services via personal equipment in unauthorized

locations such as the home of the collaborator or contractor, and with technology not approved by ETA, such as Yahoo!, Gmail, Hotmail, or other emails services is prohibited.

- Do not leave files open and unsupervised at any time. The custodian of the files is responsible for safeguarding the information contained therein.
- Do not leave the computer unattended at any time. You must lock it to step away momentarily.
- Records containing PII must be in a secure file or place with restricted access or in locked cabinets when you are not using them or when you step away from your work area.
- **Locked boxes will be used to transfer the files and all documents containing participants' PII while maintaining security and confidentiality.**
- **It is prohibited to include the social security number in: application forms, letters, memorandums, forms, among others.**
- The reproduction of PII for personal benefit or that of third parties with the intention of harming in any way the participant or the interests of AMSI is prohibited.
- Confidential information may be offered, reproduced, disclosed or shared only with a written authorization of the affected party (AMSI-2018 P/124 Participant Waiver of Responsibility), and under the following circumstances:
    - When the information is requested by the Municipal, State or Federal Government and for official or legal purposes.
    - When non-disclosure presents a risk to the health or safety of AMSI's general public.

- When this information is requested by a court order for the investigation of possible violations of Municipal, State, or Federal Laws.
- When necessary for the coordination of administrative activities, complaint management, budget management, and filing of reports to regulatory agencies.
- To determine needs and complete the processing of the requested services.
- For purposes related to the evaluation of applications for employment or unemployment.
- To manage services with other private organizations and public agencies pertinent to the case, as long as the participant is properly informed in this regard.
- To compile the necessary information in the mechanized information system.

- Report immediately any breach or suspected violation to the federal officer in charge and to ETA Information Security at ETA.CSIRT@dol.gov; (202) 693-3444, and follow the instructions received from the ETA officers.

E. Disposition of Documents and Information

- In the destruction of sensitive PII files, appropriate methods such as shredding or incineration will be used; as well as secure methods to discard sensitive electronic PII.
- AMSI will keep the personal information contained in the files, records, and systems including the data received from the ETA during a set retention period, as stipulated by the applicable law or regulation. When the time is due, all the data will be removed, including the degaussing of magnetic tape files and the deletion of electronic data in accordance with the applicable document disposition procedures and the terms provided by Law No. 5 of

December 8, 1995 (as amended), known as the Puerto Rico Public Records Administration Act.

F. Compliance

• Collaborators who have access to sensitive, confidential, and private data of the participants, must keep said information strictly confidential during its handling.

• This confidentiality is guaranteed by the federal and state laws that protect such data. If collaborators fail to comply with these regulations, they will be exposed to the corresponding civil and criminal sanctions.

• The provisions of this procedure will be faithfully fulfilled by all AMSI Collaborators; including regular employees, irregular employees, transitory or contract employees, and trusted personnel.

G. Non-compliance

- Failure to comply with this procedure, in any or all its parts, as well as the use or disclosure of PII for an unauthorized purpose, could result in the termination or suspension of related funding or the imposition of special restrictions or conditions for AMSI.

- AMSI may impose the necessary disciplinary actions on Collaborators who fail to comply with the foregoing, including termination of employment, depending on the seriousness of the offense, and as established in the Human Resources Regulations of AMSI, Inc., (revised).

H. Approval and Validity

Amendment II to the Personal Identifiable Information (PII) Management and Protection Procedure is approved today, **April 28, 2021**, in Caguas, Puerto Rico.

Ana G. Arias Villasuso
Associate Administrator
Research and Development Division
Executive Administration Area

Joaquín Santiago Santos
Executive Administrator

Vicky Cintrón de Azize
President
Local Labor Development Board