work systems	**Organization Policy ☒** **Standard Operating Procedures ☒**	
Topic: Personally Identifiable Information		
Date: July 1, 2025	**❒ New ☒ Revised**	

Purpose

The purpose of this policy is to establish guidelines and instruction for Worksystems' staff related to the protection of Personally Identifiable Information (PII) in carrying out official duties for the workforce system regardless of the location of the work (in office, remote or any other location).

Contents

Overview

As part of grant activities, Worksystems' staff and subrecipients (including WIOA service providers) may have in their possession large quantities of Personally Identifiable Information (PII) relating to their organization and staff; partner organizations and their staff; and individual program participants. This information is generally found in personnel files, participant data sets and files, performance reports, program evaluations, grant and contract files and other sources. All parties in possession of PII are required to take aggressive measures to mitigate the risks associated with the collection, storage, and dissemination of PII.

Definitions

The US Department of Labor (DOL) has defined two types of PII, protected PII and non-sensitive PII. The differences between protected PII and non-sensitive PII are primarily based on an analysis regarding the "risk of harm" that could result from the release of the PII.

- Protected PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual and that if disclosed could result in harm to the individual whose name or identity is linked to that information. Examples of protected PII include, but are not limited to, social security numbers, credit card numbers, bank account numbers, home/cell telephone numbers, ages, birthdates, marital status, spouse names, educational history, biometric identifiers (fingerprints, voiceprints, iris scans, etc.), medical history, financial information and computer passwords.

- Non-sensitive PII is information that if disclosed, by itself, could not reasonably be expected to result in personal harm; it is stand-alone information that is not linked or closely associated with any protected or unprotected PII. Examples of non-sensitive PII include information such as first and last names, business addresses, business telephone numbers, general education credentials, gender or race.

  Depending on the circumstances, a combination of more than one non-sensitive PII items could potentially be categorized as protected PII. To illustrate the connection between non-sensitive PII and protected PII, the disclosure of a name, business e-mail address, or business address most likely will not result in a high degree of harm to an individual. However, a name linked to a social security number, a date of birth, and/or mother's maiden name could result in identity theft.

Policy

- Confidential PII records include entire record systems, specific records or individually identifiable data that are not subject to public disclosure under Oregon Revised Statutes 192, and may include all documents, participant files, computer files, letters, and other notations of records or data.
- Worksystems staff access to confidential data must be limited to only those needing access to the information to perform their official duties. Although staff may be authorized to access confidential data, they may access the data only in connection with the performance of their official duties and after having signed any required confidentiality agreements.
- Worksystems staff who have access to PII must be advised of the confidential nature of the information, the safeguards required to protect the information and that there are civil and criminal sanctions for noncompliance with such safeguards that are contained in Federal and State laws.
- All PII data must be processed in a manner that protects the confidentiality of the data and is designed to prevent unauthorized persons from retrieving the data by computer, remote terminal or any other means. To ensure that such PII is not transmitted to unauthorized users, all PII and other sensitive data transmitted via e-mail, mobile or portable devices, or stored on CDs, DVDs, thumb drives, etc., must be encrypted using a Federal Information Processing Standards (FIPS) 140-2 compliant and National Institute of Standards and Technology (NIST) validated cryptographic module. In addition, wage data may only be accessed from secure locations.
- Worksystems' subrecipients must have written PII policies and procedures in compliance with TEGL 39-11.

Storage and Sharing of PII

- Participant information is stored in the I-Trac database, managed by Worksystems. Access to I-Trac is restricted to individuals who have successfully completed I-Trac User and Confidentiality Training.
- I-Trac reports that contain PII or sensitive data and are downloaded from I-Trac and other reports containing participant PII or sensitive information may not be shared with anyone not authorized to receive the information.

- Paper documents that contain PII must be stored in a confidential, locked file cabinet that is physically safe from access by unauthorized people. Paper documents that contain PII must not be left unattended.
- PII data must be stored in an employer managed cloud storage or employer managed network drive, or it must be managed within a Worksystems or employer authorized database. PII must not be saved directly on computer hard drives or mobile devices.
- Computers must be password protected and must be locked when not in use and anytime a staff person is away from their computer.
- All mobile devices must be password protected to conduct any business operations and must be locked when not in use.
- Users will not open files containing PII or login to participant databases from public wi-fi networks.
- The use of photography in areas with PII and other sensitive information in view is prohibited.

Sharing PII and sensitive information must be done following one of the secure sharing options outlined below.

Procedures for Sharing PII

Secure Sharing Options

When sharing participant information that includes PII or sensitive information that is required by a funder or to manage a program overseen by Worksystems, it must be done via one of the below secure options.

Use of encrypted email or the I-Trac File Exchange protects the data in transit, but staff lose the ability to protect the data once it is in the recipient's hands. This should be carefully considered before sharing data and a determination made that the PII or sensitive data is necessary to the recipient completing their work or a funder requirement.

Encrypted Email Message

Encrypting an email message means it's converted from readable plain text into scrambled cipher text. Only the recipient who has the private key that matches the public key used to encrypt the message can decipher the message for reading. Staff or Contractors must not email unencrypted sensitive PII to any entity including internal emails within the organization. Check with your IT Administrator for instructions to encrypt emails.

I-Trac

Documents can be sent securely through I-Trac utilizing the Secure File Exchange or the Customer Documentation Upload tool.

- **Secure File Exchange** is a way I-Trac users can exchange sensitive documents securely with each other. Documents can only be shared with other current I-Trac users. Files shared are available for the recipient to download for up to 5 business days. The recipient will receive an email that a file has been uploaded for them to retrieve. Access the I-Trac Secure File Exchange by logging into I-Trac, go to the Resources Tab - File Exchange Tab.

- **Customer Documentation Upload** is a way to upload sensitive documents that need to be attached as backup documentation to a participant's record. These documents are generally eligibility or performance documents. Documents uploaded are reviewed and then locked for security reasons. They cannot be seen by general users following review and they cannot be downloaded. For more information and instructions to use this tool, log in to I-Trac and go to Resources Tab - User Instructions Tab and open the Customer Documentation Upload manual.

Security Violation / Breach

A breach occurs when any unauthorized individual or entity gains access to personal information or when unintended disclosure of personal information is made, for example loss or theft of an electronic device containing personal information, loss or theft of a paper document containing personal information, unauthorized access to a network containing personal information, or a document containing personal information being sent to the wrong address.

Security Violation/ Breach Procedures

Breaches involving PII must be immediately reported via email, but no later than twelve (12) hours after discovery of the breach, to Worksystems at support@i-trac.org with a copy to their Worksystems Manager. The email must include a brief description of the security breach, the type of security breach (e.g., electronic, data systems, paper files), the steps taken to address the security breach and the contact names of the staff member that Worksystems is to work with responding to the security breach.

If a device is lost/stolen, passwords must be reset immediately for all devices and accounts that access the work information.

The staff member must agree to fully cooperate with Worksystems in Worksystems' participation in the matter, including, without limitation:

- Conducting or assisting with any investigation.
- Providing Worksystems with physical access to the facilities and operations affected.
- Performing or facilitating interviews with staff and others involved in the matter.
- Reviewing or making available all relevant records, logs, files, data reporting, and other materials required to comply with Applicable Laws, Best Industry Practices, or as otherwise required by Worksystems.
- Maintaining and preserving all documents, records, and other data related to the security breach.

PII Record Retention and Destruction

All PII records must be retained and commercially shredded and destroyed on or after the Disposition of Records date reflected on the schedule in the *Record Retention and Destruction Regional Program Standards*.

References

TEGL 39-11 Handling and Protection of Personally Identifiable Information (PII)
CCWO OED Joint Policy; Confidentiality and Access to Information and Data
Oregon Revised Statutes 192.001, §162.425, 657.665, §676.177, §660.339
Oregon Administrative Rules 471-010-0105, 589-020.0320, 589-020-0330