

	<b>Subject</b> Protected Personally Identifiable Information (PII) Policy ARIZONA@WORK-Yuma County	
	<b>Effective Date</b> June 14, 2023	<b>Revision Date</b>
	<b>Approved by:</b> Yuma County Workforce Development Board	

**Purpose:**

This policy provides guidance in handling Protected and Sensitive Personally Identifiable Information (PII).

**Scope:**

To protect client data entrusted to ARIZONA@WORK-Yuma County AKA the Yuma Private Industry Council.

**Policy:**

**Requirements:** To follow and satisfy the requirements of TEGL 39-11 and all applicable laws. [https://www.dol.gov/sites/dolgov/files/ETA/advisories/TEGL/2012/TEGL\\_39\\_11.pdf](https://www.dol.gov/sites/dolgov/files/ETA/advisories/TEGL/2012/TEGL_39_11.pdf)

To safeguard Protected PII, the Agency will require staff and partners to abide by this Policy. The requirements of this Policy include:

**Acknowledgement:** All Staff and Partners will be required to read and understand TEGL 39-11, and agree in writing to comply with the requirements therein.

**Collection of PII:** All Staff and Partners shall collect only Sensitive or Protected PII which is necessary to determine program eligibility. Collection can be performed in-person, by upload into a secure document storage system (ISDS/AJC) or by Virtru encrypted email.

**Handling of PII:** All Staff and Partners will safeguard Sensitive and Protected PII. Only Authorized Staff shall have access to any document storage system (file cabinets/ISDS/AJC), email, desktop files, or documents for scanning. Photocopies shall be destroyed immediately after use.

**Storage of PII:** All Staff and Partners will ensure that Sensitive or Protected PII shall not be stored on Agency workstations, personal computing devices, phones, non-encrypted external storage devices, cloud storage (Google Workspace, Microsoft One Drive, etc) or other non-approved method. The only approved storage methods for Sensitive or Protected PII are AJC/ISDS and on-site, IT-managed storage (Y drive).

**Transfer of PII:** All Staff and Partners will ensure that Sensitive or Protected PII is transferred only to authorized users. Transfer may be accomplished via the ISDS/AJC system, Virtru secure email, encrypted storage devices (USB storage device, et al) or person-to-person.

**Retention of PII:** All Staff and Partners will store Sensitive or Protected PII for only as long as necessary to fulfill the eligibility function or as required by applicable law. Storage systems shall have a “purge date” to identify documents to be purged on a regular basis.

**Auditing:** All Staff and Partners agree and understand that Federal, State or local monitors/auditors may inspect computers/storage systems for legally-allowable purposes, including inappropriate retention of Sensitive or Protected PII.

**Scope:** This Policy is intended as a statement of intent, and is not expected to be complete and thorough for every situation. The source of this document is DOL TEGL 39-11, included as an attachment, and other applicable privacy laws, including FERPA and HIPAA.

**Enforcement:** Staff and Partners found to be in violation of this policy shall be subject to disciplinary action, up to and including termination. Civil and Criminal penalties may also apply.

**Yuma Private Industry Council, Inc. (YPIC)**

**ARIZONA@WORK/Yuma County**

**Protected Personally Identifiable Information (PII) Policy**

Violation of TEGL 39-11 and the Protected Personally Identifiable Information (PII) Policy will lead to disciplinary action by the Council up to and including termination of employment. Infractions will be reported to Human Resources.

I, (printed name) \_\_\_\_\_,  
acknowledge that I have read and understand the TEGL 39-11 and the Protected Personally Identifiable Information (PII) Policy. I further understand that failure to follow the provisions of the Policy may lead to loss of IT resources and privileges. I also acknowledge and understand that, depending on the seriousness of the specific violation and / or damage caused to the Council resources that disciplinary action, up to and including termination, may be imposed. By signing below, I agree to abide by this Policy:

**Name:**

\_\_\_\_\_

**Date:**

\_\_\_\_\_

**This document will be placed in your personnel file**