Workforce Development Board

Region 9

PII Protection Policy

Effective Date: July 1, 2018

SUMMARY**:**

This policy explains the methods and responsibilities for handling Personally Identifiable Information (PII) for Southeast Indiana Workforce Development Board Staff and any individuals within the LWDA with access to Protected PII.

REFERENCES: CFR 200.82

BACKGROUND: Southeast Indiana Workforce Development Board staff, and individuals with the LWDA, are entrusted with information that must be kept secure and private. If Personally Identifiable Information (PII) documents and records are not securely stored and destroyed, there is a potential danger that the records of individuals as well as businesses can be wrongfully accessed and misused for illicit purposes, such as identity theft or fraud. All individuals, organization, business entities and staff with access to confidential and privileged customer information have an obligation to ensure the protection and appropriate business use of the information.

DEFINITIONS:

Protected PII and/or sensitive information is information 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 (SSNs), credit card numbers, bank account numbers, home telephone numbers, ages, birthdates, marital status, spouse names, education history, biometric identifiers (finger prints, voice prints, iris scans, etc.) medical history, financial information and computer passwords.

Non-sensitive PII, on the other hand, is information that if disclosed, by itself, could not reasonably be expected to result in personal harm. Essentially, it is stand-alone information that is not linked or closely associated with any protected or unprotected PII. Examples of non-sensitive PII includes information such as first and last names, email addresses, business addresses, business telephone numbers, general education credentials, gender or race. However, depending in the circumstances, a combination of these items could potentially be categorized as protected or sensitive PII. To illustrate the connection between non-sensitive PII and protected PII, the disclosure of a name, business email address or business address mostly 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 mother's maiden name could result I identity theft. This demonstrates why protecting the information of our program participants is so important.

GUIDANCE:

PII and/or sensitive information if not securely stored and shredded in accordance with this policy, can cause irreparable harm to individuals, businesses and to the Southeast Indiana Workforce Development Board. Please note that this policy does not supersede existing record retention policies or guidelines set forth by the Indiana Commissions on Public Records. PII and/or sensitive information not required to be retained for a certain period of time under Indiana Commission on Public Records policies will be shredded (and recycled, where feasible).

Employees must not store PII and/or sensitive information to be shredded underneath their desks in boxes or containers. All PII and/or sensitive information must be taken to the specified locked receptacles (where feasible) or shredded as soon as possible. Any employee who discovers PII and/or sensitive information unsecured, inappropriately filed, or not stored to prevent inappropriate disclosure must immediately notify the Executive Director.

Storage of PII and Sensitive Information

When an employee's desk is unattended, it is the employee's responsibility to ensure that PII and/or sensitive information is properly filed and stored. This means that all documents containing PII and/or sensitive information must not be left on desks, fax machines, printers, or photocopiers unattended. When not working directly with these documents, they must be filed or stored in drawers to present inadvertent disclosure of information. Examples of documents include post-it-notes, scrap pieces of paper, or files with social security numbers, names or other confidential information.

Transmission of PII and Sensitive Information

Distribution of PII is strictly forbidden, except in the limited cases in which PII is required for critical core functions (e.g. payroll and HR functions, required monitoring or audits) that are explicitly authorized by the Executive Director and performed in accordance to a staff members' roles and responsibilities. In all cases, PII can only be distributed via secure means, (e.g. encrypted emails, encrypted hard drives or thumb drives, password protection).

Additional Security Measures

The unauthorized use of cameras, including cell phone cameras, is prohibited from use at all times while PII is present. Cameras that are used for business reasons must be used with management approval and all photographs limited to the subject area. Cameras that are used in an unauthorized manner, or to collect confidential and/or privileged information, will subject the user to immediate disciplinary action.