Region 4 Workforce Development Board
Personally Identifiable Information (PII)

PURPOSE: This policy explains the methods and responsibilities for handling Personally Identifiable Information (PII) at all WorkOne Centers and WorkOne Express sites. Indiana Department of Workforce Development staff, all employees of organizations partnered in direct or indirect contractual relationships with the State of Indiana or any of its subcontracted entitled shall adhere to the requirements of this policy.

REFERENCES: 29 CFR Part 38, DWD Policy 2007-46, DWD Policy 2007-42, TEGL 39-11

BACKGROUND: The Indiana Department of Workforce Development is 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 Department 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.

CONTENT:
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 Indiana Department of Workforce Development. Please note that this policy does not supersede existing record retention policies or guidelines set forth by the Indiana Commissions on Public Records. According to Commission's policies, many IDWD records must be retained for a certain number of years, such as those of the Trade Adjustment Assistance program, Unemployment Insurance claims, Unemployment Insurance tax and basic accounting 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 a supervisor who will then contact the IDWD Investigations/Security Section.

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. Regulations in the Health Insurance Portability and Accountability Act (HIPAA) (http://www.cms.hhs.gov/hipaa/) limit the way in which personal health information is disclosed. Health subjects include mental and behavioral health. Such information gathered should not be added into case notes, but stored in a separate file.

Additional Security Measures

The unauthorized use of cameras, including cell phone cameras, is prohibited from use at all times while on WorkOne or Department premises. Cameras that are used for business reasons or to document special occasions, such as retirements and birthday parties, 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.

Effective: July 2018

INDIANA DEPARTMENT OF WORKFORCE DEVELOPMENT
Indiana Career Connect Staff Account Application
Indiana Career Connect Case Management/Labor Exchange System Acceptable Use and Confidentiality Policy

It is the responsibility of all authorized Indiana Career Connect(ICC) users, (which may include but is not limited to the following: Case Managers, Department of Workforce Development Staff, Regional Workforce Board Staff, Service Provider Staff, and Regional Operator Staff), to safeguard sensitive client information. This information includes all personal information obtained from those seeking assistance from the WorkOne system and its affiliates. Unless otherwise identified by DWD management, all client information entered into the ICC system is confidential and is not to be shared or disclosed to organizations, agencies or individuals outside the Indiana Department of Workforce Development, its authorized representatives/agents, the Department of Labor and/or its authorized representatives/agents, agencies or organizations within the scope of those authorized by the Client's Release forms, partner MOUs, and/or other affidavits insuring confidentiality of records, and which relate to the provision of employment, support, and training services.

One of the primary objectives under Indiana's State Plan is integrated delivery for the overall benefit of the customer. The new mandatory statewide case management/labor exchange system, ICC, is designed to support that objective by allowing for a shared case management process. ICC allows authorized users to view information on all clients who are entered into the system across the state. This information includes case notes, with the exception of those relating to domestic violence, which are required to be "locked down" in the system.

Staff entering case notes should enter complete information needed to support the employment plan, but should refrain from entering any information that is not relevant to the employment plan or that is overly graphic and/or non-essential.

This confidentiality policy will be strictly enforced: Violators will face disciplinary actions that could result in termination of employment.

I have read and understand the above ICC Case Management/Labor Exchange System Acceptable Use and Confidentiality Policy, and agree to its terms.

Please print pages, complete all fields, scan pages into PDF and send to R4WDB Elite User.

_____	_____	_____
User Signature	Supervisor Signature	Date (MM/DD/YYYY)