EmployIndy
GUIDING MARION COUNTY'S WORKFORCE

POLICY OF EMPLOYINDY

Policy Name	Information Security and Confidentiality
Policy Number	2015-028
Program Funding Stream	All

REV	Description of Change	Author	Approval Date	Effective Date	Review Date
	Reissued and replaces policy #2010-SD-001; Information Security	S. Phillips		Upon Approval	12/31/16
1	Extended Review Date.	S. Johnson		Upon Approval	5/31/2018
2	Added requirements for if a data breach occurs.	O. Volokhova		5/15/2018	5/1/2019
3	Added monitoring, information disclosure, discipline, among other various clarifications	K. Duffy	10/~~1~~8/2018	10/24/2018	10/24/2019
	WorkOne Indy requirements			1/1/2019	10/24/2019

1. Purpose

To establish a policy for the protection of personally identifying information (PII) as well as information that is confidential or privileged that is generated, collected, and/or utilized by the EmployIndy system, and to outline the corrective action should an unauthorized disclosure occur.

2. Scope

This policy applies to all EmployIndy and service provider staff members when handling confidential and/or privileged information generated, collected, and/or utilized during the course of EmployIndy program operations.

3. Summary of the Law, Rules, and Governing Policies

Indiana Code 24-4.9-3 describes required actions for organizations to undergo if a security breach results in a participant's personal information being improperly disclosed.

DWD Policy 2013-03: Requirements Pertaining to Confidential and Privileged Information provides guideline and requirements for the appropriate use, storage, and access of confidential and/or privileged information maintained by DWD or any entity providing customer services connected to or through the WorkOne system.

TEGL No. 3911: Guidance on the Handling and Protection of Personally Identifiable Information (PII) provides guidance to WIOA grantees on compliance with the requirements of handling and protecting PII.

4. Responsibilities

EmployIndy directors are responsible for oversight and implementation of this policy, and for ensuring their staff adhere to this policy. The EmployIndy Director of Career Services is responsible for implementing WorkOne-specific requirements at WorkOne Indy locations.

Service provider managers are responsible ensuring their staff adhere to this policy, and for ensuring that the required information described in this policy is sent from the service provider to EmployIndy.

The EmployIndy staff contract owner is responsible for collecting the information required from service providers under this policy and distributing it to the following staff:

- EmployIndy Director of Quality and Analytics and the EmployIndy Manager of Policy, who are responsible for determining whether the information provided satisfies the policy requirements.
- EmployIndy Grants and Contracts Manager, who is responsible for attaching the information to the service provider's contract as a binding document once approved.

The EmployIndy Quality and Analytics Department is responsible for annual monitoring of service providers for compliance with this policy.

The Director of Quality and Analytics is responsible for ensuring proper steps are taken in the event of data breach.

5. Policy Statement

The following requirements apply to all EmployIndy staff and service provider staff when handling confidential and/or privileged information generated, collected, and/or utilized in the course of EmployIndy program operations.

Access to Confidential and/or Privileged Information
Access to confidential and/or privileged information must only be granted to staff for legitimate business purposes.

Electronic Usage, Storage, and Transmission
All confidential and/or privileged information stored or transmitted electronically must be secured through password protection, either by requiring a password to access the device when locked or by requiring a password to access the documents containing confidential and/or privileged

information.[1] Information containing sensitive PII must be redacted or encrypted before being transmitted electronically.

Non-public electronic devices used for WorkOne Indy or EmployIndy business purposes must be locked when not in use.

When confidential and/or privileged information containing sensitive PII is being faxed, the sensitive PII must either be redacted or the sender must confirm that the receiver will be present to receive the fax.

Passwords to electronic devices and accounts issued or owned by EmployIndy or WorkOne Indy must be changed, at a minimum, every 3 months.

Physical Storage

Confidential and/or privileged information must not be posted, displayed, or left exposed and unattended. When not in use, hard copies of confidential and/or privileged information must be secured and locked.

Confidential and/or privileged information must be secured whether being stored at a worksite or off-site location. Supervisors must have prior knowledge and consent before any confidential and/or privileged information may be removed from its approved storage place.

Documents containing confidential and/or privileged information must be shredded prior to disposal.[2]

Training

All EmployIndy and service provider staff members must be informed at hire of the requirements in this policy and trained at least annually on these requirements.

EmployIndy and service provider managers must ensure their staff are trained on rules and procedures governing systems used in the course of their job responsibilities. Staff must follow all rules and procedures governing systems used in the course of their job responsibilities. If there exists a conflict between information security requirements laid out by a system owner and those contained in this policy, the more stringent of the two must be followed.

Employee Offboarding

Network passwords must be deactivated and changed within 24 hours of an EmployIndy or service provider staff member who has knowledge of the passwords terminating employment.

WorkOne Indy and/or EmployIndy keypads and locked doors must have the access codes deactivated and changed within 24 hours of any employee who has knowledge of the access code terminating employment.

Unauthorized Disclosures

The requirements above are intended to ensure that a participant's information is not accessed or disclosed by an unauthorized individual.

[1] See "WorkOne Indy Requirements" for additional requirements for WorkOne Indy employees electronically transmitting information containing PII.
[2] See EmployIndy *Records Retention and Document Destruction* Policy

An improper disclosure occurs when an individual's personal information is shared with an individual or entity that is not an EmployIndy staffer or service provider or if shared outside of the terms of a contract or memorandum of understanding (MOU) or Data Sharing Agreement (DSA) for data sharing.

EmployIndy must also notify the affected individual "without unreasonable delay."[3] A delay is reasonable if it is necessary to restore the integrity of the computer system or is necessary to discover the scope of the breach.[4]

If an EmployIndy staff member or service provider staff member inadvertently discloses a client's personal information to an unauthorized party, the individual must immediately notify EmployIndy's Director of Quality and Analytics or designee. Upon receipt of the notification, the Director of Quality and Analytics must take the following steps:

1. Determine as soon as possible whether a breach occurred.
2. Notify the Chief Operating Officer, all EmployIndy Directors, and other applicable staff of the breach.
3. Contact the IT service provider regarding the breach, if applicable.
4. If a breach occurred, restore the integrity of the system to ensure no further breaches occur and discover the scope of the breach.
5. After restoration and discovery, notify the affected individual or individuals and notify the Office of the Attorney General using the Indiana Data Breach Notification Form.[5] EmployIndy may offer credit monitoring at no cost to the participant.

Discipline

EmployIndy staff members who knowingly access and/or use confidential and/or privileged information beyond the scope of authority granted or without legitimate business reason to do so will be subject to immediate corrective action, up to and including termination of employment.

In the event a service provider employee administering an EmployIndy program knowingly accesses and/or uses confidential information beyond the scope of authority granted or without legitimate business reason to do so, EmployIndy reserves the right to withhold from that service provider funding for the employee's position until the employee is removed from their position administering an EmployIndy-funded program.

WorkOne Indy Requirements

The following requirements apply to WorkOne Indy staff and locations only:

- Confidential and/or privileged information containing sensitive PII transmitted electronically or stored on an external storage device must be encrypted using a FIPS 140-2 compliant and NIST validated cryptographic module.[6]
- WorkOne Indy employees must sign an Acknowledgement Release that they have read DWD Policy 2013-03 as well as TEGL No. 39-11 and agree to use confidential and privileged information for authorized work-related purposes only and to abide by all other requirements and terms therein.[7] This requirement may be satisfied by having new

[3] I.C. § 24-4.9-3-1
[4] I.C. § 24-4.9-3-3
[5] https://www.in.gov/attorneygeneral/files/841375_1(1).PDF.
[6] http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
[7] DWD Policy 2013-03

employees sign State Form 54116, Acknowledgement of Agency Policies and Procedures (Attachment A), as part of the hiring process.

- The following guidelines governing the use of cameras at WorkOne Indy offices must be followed:
    - Unauthorized use of cameras is prohibited from use at all times while on WorkOne Indy premises.
    - Cameras used for business reasons or to document special occasions must be granted approval by the EmployIndy Director of Career Services or designee and limited to the subject area.
    - Cameras used for media purposes must receive prior approval from DWD.
    - Use of cell phone cameras is discouraged.

Information to be provided by service providers

When responding to an EmployIndy service provider RFP, all applicants must give a description of information security and confidentiality practices and policies currently in place for that entity.

Each contract executed between EmployIndy and a service provider must require the service provider to provide the following information to EmployIndy within 90 days of execution[8]:

- The designated staff person(s) responsible for informing EmployIndy when an employee is terminated.
- A training schedule indicating when staff will be trained on the requirements in this policy; training must be conducted at hire and at least annually afterward.

All existing service provider contracts must be modified to include this requirement.

The EmployIndy contract owner must be responsible for collecting this information by the date specified in the contract and delivering copies to the EmployIndy Grants and Contracts Manager, Director of Quality and Analytics, and the Manager of Policy. The Director of Quality and Analytics and Manager of Policy must determine whether the information provided satisfies the requirements in this policy.

Monitoring

The EmployIndy Quality and Analytics Department must annually monitor service providers and offer technical assistance to ensure compliance with this policy.

6. Exceptions

Any exception to this policy must be approved by an Executive Team Member.

7. Definitions

Confidential information: Information that has been designated by statute or by promulgated rule or regulation based on statutory authority.

EmployIndy System: Service Providers, individuals conducting business with an AJC location, EmployIndy staff and individuals working within any EmployIndy contracted service provider locations.

[8] Extensions may be granted on a case-by-case basis with EmployIndy Department Director approval.

Personally Identifiable Information (PII): Any 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. There are two types of PII: Protected, and Non-sensitive.

- Protected PII is information that if disclosed could result in harm to the individual whose name or identity is linked to that information.
- Non-sensitive PII is information that if disclosed, by itself, could not reasonably be expected to result in personal harm. Depending on the circumstances, a combination of these items could potentially be categorized as protected or sensitive PII.

Personal information: This definition is used in the context of a data breach and subsequent required disclosure to the Indiana Attorney General. Means an unredacted or unencrypted Social Security number, or an individual's first and last names, or first initial and last name, and one or more of the following data elements that are not encrypted or redacted:

- A driver's license number
- A state identification card number
- A credit card number
- A financial account number or debit card number in combination with a security code, password, or access code that would permit access to the person's account.

This term does include information that is lawfully obtained from publicly available information or from government records lawfully made available to the general public. Personal information is considered redacted if no more than five digits of a Social Security number or four digits of the following are accessible:

- A driver's license number
- A state identification number
- An account number[9]

Privileged information: Information which is available only to authorized persons and is gained access to by one's position or through partnership in contractual relationships with EmployIndy or the Department of Workforce Development.

8. Related Policies and Documents

Policies:

EmployIndy *Computer and Equipment Usage* Policy[10]
Indiana Department of Workforce Development, "DWD Policy 2013-03: Requirements Pertaining to Confidential and Privileged Information."[11]

[9] IC 24-4.9-2-10
[10] https://employindy.org/wp-content/uploads/2017/08/7-1-Computer-and-Equipment-Usage.pdf
[11] http://www.in.gov/dwd/files/DWD_Policy_2013-03.pdf