SOP 15-09
Requirements Pertaining to Confidential and Privileged Information
Standard Operating Procedures
Grow Southwest Indiana Region 11
Approval Date: 09/27/2013

Purpose

To establish guidelines and requirements for the appropriate use, storage, and access of Confidential and/or Privileged Information maintained by the Indiana Department of Workforce Development ("Department") and/or any entity providing customer services connected to or through the WorkOne system.

Rescission

DWD Policy 2007-45, "Requirements Pertaining to Confidential and Privileged Information," issues June 28, 2008.

Action

DWD Policy 2013-03 Requirements pertaining to Confidential and Privileged Information will be implemented in Region 11 as SOP 15-08.

CONTENT

All individuals, organizations, business entities, and Department staff with access to Confidential and/or Privileged Information have an obligation to ensure the protection and appropriate business use of the information. This policy provides a definition for Confidential and Privileged information and specifies the requirements for the use, storage, and access to this information.

State employees and those who have a business relationship with the Department are subject to the Indiana Code of Ethics. These ethics rules and the Indiana Code of Ethics apply to any entity, organization, or individual providing customer services connected to or through the WorkOne system. The ethics rules prohibit those subject to the rules from benefiting from, or permitting any other person to benefit from, information confidential in nature and from divulging Confidential Information. A complete copy of the ethics rules may be found at http://www.in.gov.ig.

Definitions

Confidential Information

Confidential Information is that which has been so designated by statute or promulgated rule or regulation based statutory authority. Information and records of the Department relating to the unemployment tax, or the payment of benefits, including that which may reveal the individual's or the employing unit's identity, are confidential pursuant to IC 22-4-19-6(b).

Privileged Information

Personally Identifiable Information (PII) is 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. Both Confidential Information and Privileged Information may contain PII. PII can be further delineated as Sensitive PII (or Protected PII) and Non-Sensitive PII. See Training and Employment Guidance Letter (TEGL) No. 39-11.

Sensitive PII, or Protected PII, is any information that if disclosed could result in harm to the individual whose name or identity is linked to that information. Examples include, but are not limited, to social security numbers, credit card numbers, bank account numbers, personal telephone numbers, ages, birthdates, marital status, spouse names, educational history, 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. Examples include, but are not limited to, first and last names, general education, credentials, gender, or race. However, depending on the circumstances, a combination of those items could potentially be categorized as Protected or Sensitive PII.

State Property

All information including but not limited to documents, software, files, and e-mail, created, accessed, transmitted, or stored, electronically or in paper form while employed by or partnered

in contractual relationships with the State of Indiana or any of its subcontracted entities shall be considered the exclusive property of the State of Indiana.

Data Security Requirements

Storage of Confidential and/or Privileged Information

When an employee's desk is unattended, it is the employee's responsibility to ensure that Confidential and/or Privileged Information, including that containing PII, is properly filed and stored. This means that all documents containing Confidential and/or Privileged 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 prevent inadvertent disclosure of information.

Access to Confidential and/or Privileged Information

Employees may only access Confidential and/or Privileged Information, including that containing PII, to the extent they have permission and/or authority to access it. Accessing, processing, and storing of any data containing PII on personally owned equipment, at off-site locations, e.g. employee's home, and non-grantee managed IT services, e.g. Yahoo mail, is strictly prohibited unless otherwise approved by the Department. Wage data may only be accessed from secure locations.

Electronic Data

Any and all Confidential and/or Privileged Information containing PII transmitted via e-mail or stored on CDs, DVDs, thumb drive, mobile or portable devices, etc. must be encrypted using a Federal Information Processing Standards (FIPS) 140-2 compliant and National institute of Standards Technology (NIST) validated cryptographic module. WorkOne employees or Department staff are prohibited from e-mailing unencrypted Confidential or Privileged Information containing Sensitive PII to any person or entity. TEGL 39-11.

Additional Security Measures

The unauthorized use of cameras, including cell phone cameras, is prohibited from use at all time 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.

Security Breach

Any WorkOne employee and Department staff who becomes aware of any security breach resulting from the inadvertent or intentional leak or release of Confidential and/or Privileged Information, including that containing PII, shall immediately inform their direct supervisor as well as the General Counsel of the Department.

Violation of Data Security Requirements

WorkOne employees and Department staff that fail to abide bye storage and filing requirements listed herein for Confidential and/or Privileged Information, including that containing PII, may be subject to disciplinary action.

WorkOne employees and Department staff that access and/or use Confidential and/or privileged Information, including that containing PII, beyond the scope of the authority granted or without legitimate business reason to do so will be subject to immediate disciplinary action, up to and including termination of employment.

In addition, a person who knowingly or intentionally exerts unauthorized control over the property of another commits criminal conversion, which is a Class A misdemeanor under IC 35-43-4-3(a). Therefore, WorkOne employees and Department staff who take State electronic or paper records off work premise to be utilized for personal reasons can expect to be charged with committing criminal conversion.

Failure to adhere to any other requirements or terms of this release may result in disciplinary action.

Acknowledgement Release

All WorkOne employees and Department staff shall sign an Acknowledgement Release that they have DWD Policy 2013-03 as well as TEGL No. 39-11 and agree to use Confidential and/or Privileged Information, including that containing PII, for authorized work-related purposes only and to abide by all other requirements and terms contained therein.

If an employee has signed State Form 54166, acknowledgement of Agency Policies and Procedures, as art of the hiring process at the Department, that will satisfy the Acknowledge Release requirement of this policy. State form 54166 may be found at http://www.in.gov/spd/2599.htm.

All WorkOne Centers and WorkOne Express sites and Indiana Department of Workforce Development staff shall adhere to the requirements of this policy. All employees of organizations partnered in direct or indirect contractual relationships with the State of Indiana or any of its subcontracted entities shall adhere to the requirements of this policy.