SOP 08-11
Document Shredding,
Requirements for Confidential and Privileged Information and Guidance on proper handling of Social Security Numbers
Standard Operating Procedures
Grow Southwest Indiana Region 11
Approval Date: 02/25/09

Purpose

To communicate to all Region 11 service providers the methods and responsibilities for the shredding of confidential documents, requirements for the appropriate use, storage and access of confidential and/or privileged information maintained, and provide guidelines to all WorkOne staff on the proper handling of Social Security numbers (SSNs) to prevent unauthorized access, disclosure, and possible misuse or abuse of SSNs.

Contents

Shredding of Confidential Documents

- ✓ Confidential documents to be shredded shall not be discarded in trash bins, recycling containers or other publicly assessable locations. Locked receptacles solely designated for shredding paper records are located at each location. Employees are responsible for physically taking all confidential documents to be destroyed to the locked receptacles. Cleaning crews will no longer be responsible for picking up confidential documents to be shredded.

- ✓ Employees must not place their personal paper documents into the containers to be shredded. These containers are for confidential information.

- ✓ Employees must not store confidential documents to be shredded underneath their desks in boxes or containers. All confidential documents must be taken to the specified locked receptacles as soon as possible.

- ✓ When an employee's desk in unattended, the desk must be cleared of all confidential information to prevent wrongful access, theft or fraud. Confidential information must be properly filed or stored to prevent inappropriate disclosure of information.

- ✓ Any employee who discovers confidential 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.

Requirements Pertaining to Confidential and Privileged Information

All individuals, organizations, business entities and DWD staff with access to confidential and privileged customer 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 Indiana Department of Workforce Development, 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. For a complete copy of ethics rules, visit http://www.in.gov/ig

Definitions

Confidential Information

Confidential information is that which has been so designated by statute or by promulgated rule or regulation based on statutory authority. Records of the Department relating to the unemployment tax or the payment of benefits are confidential pursuant to IC 22-4-19-6(b).

Privileged Information

Privileged information is that which is available only to authorized persons and is gained access to by one's position within DWD or through partnership in contractual relationships with the State of Indiana or any subcontracted entity funded in whole or in part by DWD grants/contracts. This information is not confidential pursuant to the law, but is sensitive in nature. Privileged information is subject to the same restrictions as confidential information for the purposes of this policy.

State Property

All information including but not limited to documents, software, files, and email, 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.

Requirements

Storage of Confidential and/or Privileged Information

When an employee's desk in unattended, it is the employees' responsibility to ensure that confidential and/or privileged information 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 can only access confidential and/or privileged information to the extent they have permission and/or authority to access it. Accessing confidential and/or privileged information beyond the scope of the authority granted or without legitimate business reason to do so will be deemed a violation and is subject to discipline up to and including termination of employment.

Unauthorized Control of Confidential and/or Privileged Information
WorkOne employees and DWD staff who take State electronic or paper records off work premises to be utilized for personal reasons may commit criminal conversion as outlines in IC 35-43-4-4 (a). A person who knowingly or intentionally exerts unauthorized control over property of another commits criminal conversion, a Class A misdemeanor.

Additional Security Measures
The unauthorized use of cameras, including cell phone cameras, is prohibited from use at all times while on WorkOne or DWD 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.

Guidance on the proper handling of Social Security Numbers to prevent possible abuse
The Guidelines are to insure the proper handling of Social Security Numbers to prevent unauthorized access, disclosure, and possible misuse or abuse of SSNs.
In the normal practice of conducting business, each WorkOne office and the DWD Administrative office collect and maintain SSNs through a variety of electronic and paper information resources. The policy applies to a SSN whether maintained, used or displayed wholly or in part, and in any format, including but not limited to oral or written words, screen display, electronic transmission, stored media, printed material, facsimile or any other medium.

Definition of Social Security Number
The number of a particular individual's Social Security account which may be interpreted to also be defined as a Taxpayer Identity Number (TIN).

Requirements for the Protection of Social Security Numbers

- ✓ Full SSNs shall be removed from all paper forms and faxes unless required by law or when dissemination is crucial to conducting WorkOne or Department business.

- ✓ Employees shall not disclose Social Security numbers to unauthorized persons or entities.

- ✓ Employees shall not seek out, sell or use Social Security numbers relating to others for their own interest or advantage.

- ✓ Employees shall not leave voicemail messages that contain full SSNs.

- ✓ Employees shall immediately report to their supervisors any inappropriate disclosure of Social Security numbers.

- ✓ Employees shall make every effort to ensure that documents containing SSNs are secured.

- ✓ Computer applications requiring SSNs must be stored on a secure network server.

- ✓ Employee notes and documents containing SSNs, which are not subject to the record retention policy, must be shredded.

- ✓ All documents and employee notes containing SSNs must not be left on desks, fax machines, printers or photocopiers unattended. All documents must be securely and properly filed or stored to prevent inappropriate disclosure of information when not in active use.

- ✓ All WorkOne staff and Administrative office staff shall abide by the provisions of this policy and shall act to ensure the security of Social Security numbers.

Legal Ramification
An employee of a state agency who negligently discloses a Social Security number commits a Class A infraction. IC § 4-1-10-10. However , an employee of a state agency who knowingly, intentionally, or recklessly discloses a Social security number commits a Class D felony. IC § 4-1-10-8.

Action
All WorkOne Centers and WorkOne Express sites and IDWD 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.