SPOKANE WORKFORCE COUNCIL

DATA PRIVACY AND SECURITY

Spokane WorkSource System Policies and Procedures
POLICY #WS823 **Effective Date:** July 1st, 2024

1. Background

Recipients of Workforce Innovation and Opportunity Act (WIOA) Title I, WIOA Title III (Wagner-Peyser) and other Federal or state grants necessarily must collect personally identifiable information (PII) to verify, document, and enroll eligible customers and to administer and manage those programs and grants. Loss of PII can result in substantial harm to individuals, including identity theft or other fraudulent use of this information. Because subrecipients and contractors may have access to individuals' PII, it is imperative that proactive methods are implemented to ensure this critical, sensitive, personal information is always protected.

As stewards of Federal funds handling PII and other potentially sensitive and confidential information, the Spokane Workforce Council and Spokane WorkSource Campus have a responsibility to secure the use, storage, and transmission of this information, collectively referred to as data. This policy provides a framework for protecting the confidentiality, integrity, and availability of data; assessing and mitigating security risks to data; and keeping security practices current and relevant.

2. Definitions

- **Data classification:** a category of data based on the sensitivity and confidentiality requirements of the data, as specified in Office of the Chief Information Officer (OCIO) Policy 141.10, other Washington state laws, and Training and Employment Guidance Letter (TEGL) 39-11, which includes the following categories:
    - **Category 1 – Public Information:** Public information is information that can be or currently is released to the public and does not require protection from unauthorized disclosure.
    - **Category 2 – Sensitive Information:** Any information whose loss, misuse, or unauthorized access to or modification of could adversely affect the interest or conduct of the SWC, its subrecipients, or the privacy to which individuals are entitled under the Privacy act. Sensitive information is not specifically protected from release or disclosure by law. Sensitive information is generally not released to the public unless specifically requested.
    - **Category 3 – Confidential Information:** Confidential information is information that is specifically protected from either release or disclosure by law. This includes, but is not limited to:
        - **Protected PII:** Information that if disclosed could result in harm to the individual whose name is linked to that information or that can be used to distinguish or trace an individual's identity on its own. Examples of protected PII include, but are not limited to:
            - Full social security number;
            - Account number, credit or debit card number, or bank account number associated with an individual's financial account;
            - Username or email address in combination with a password or security questions and answers that would permit access to an online account;
            - Any information that, when combined with an individual's first name (or first initial) and last name, is linkable to a specific individual, including but not limited to:
                - Last four digits of a social security number;
                - Driver's license number or Washington identification card number;
                - Student, military, or passport identification number;
                - Home telephone number;
                - Age;
                - Full date of birth;
                - Spouse's name;

- Marital status;
- Educational history;
- Biometric data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual;
- Financial information or any required security code, access code, or password that would permit access to an individual's financial account, or any other numbers or information that can be used to access a person's financial account;
- Health insurance policy or identification number;
- Device or lock password or passcode;
- Private key that is unique to an individual and that is used to authenticate or sign an electronic record;

- Any information that, when combined with two or more elements of other personal information, is linkable to a specific individual, including but not limited to:
  - First name (or first initial) and last name;
  - E-mail address;
  - Business address or business telephone number;
  - General education credentials;
  - Gender;
  - Race or ethnicity;

  Note: Personally identifiable information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

- **Network infrastructure and security information:** Information regarding the infrastructure and security of computer and telecommunications networks owned or utilized by the service provider is considered confidential and consists of: security passwords, security access codes and programs, access codes for secure software applications, security and service recovery plans, security risk assessments, security test results to the extent that they identify specific system vulnerabilities, and other such information that the release of which may increase risk to the confidentiality, integrity, or availability of data or IT systems.

- **Category 4 – Confidential Information Requiring Special Handling:** Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which especially strict handling requirements are dictated through statute, regulation, or agreement and serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions. This information includes, but is not limited to:

  - Any information about an individual’s medical history, mental or physical condition, or about a health care professional's medical diagnosis or treatment of the individual, must be secured in a separate location (physical or electronic) and access must be restricted to individuals who explicitly require access to the information for agency business (see storage and sharing below);
  - Wage data obtained through state unemployment insurance records must be secured in a separate location (physical or electronic) and access must be restricted to individuals who explicitly require access to the information for agency business (see storage and sharing below);

- **Secured data:** Data encrypted in a manner that meets or exceeds the National Institute of Standards and Technology (NIST) standard or is otherwise modified so that the personal data is rendered unreadable, unusable, or undecipherable by an unauthorized person.

- **Security breach:** Unauthorized acquisition of data that compromises the security, confidentiality, or integrity of confidential data maintained by an agency. Good faith acquisition of personal data by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system when the personal data is not used or subject to further unauthorized disclosure.

- **Service provider:** A provider of workforce development services in Spokane County, such as partners located at the local one-stop center or other entity designated by the Spokane Workforce Council (SWC), that is responsible for determinations of program eligibility, documentation, self-attestation guidelines, and other eligibility and documentation requirements as defined by the SWC.

- **Trusted network:** A network that includes security controls. At a minimum, these controls must include a firewall, private access control on networking devices such as routers or switches, and antimalware software

(including antivirus). Trusted networks may also include other mechanisms which protect the confidentiality, integrity, and availability of data. Public hotspots, such as in airports and hotels, and dial-up connections, are considered untrusted networks.

3. Policy

This policy covers all data owned or obtained by service providers who handle category 3 or 4 confidential data, and information systems and resources used for the collection, processing, use, sharing, maintenance, dissemination, or disposition of data, whether digital or non-digital, owned or obtained by service providers who handle category 3 or 4 confidential data. Data includes all physical and electronic records. Information systems and resources include personnel, equipment, and information technology such as hardware, firmware, and software.

This policy applies to recipients of WIOA title I, WIOA title III, Washington state, and/or other Federal grants that require the handling of category 3 or category 4 confidential data in the Spokane WorkSource system. For the purposes of the requirements below, the term "confidential data" refers to both category 3 and category 4 data.

a. **Collection of data** – Service providers must limit the collection of confidential data to only data necessary for the administration of a program or grant or to perform their official job duties (WorkSource Policy 1026 – Safeguarding PII).

b. **Configuration and security controls** – Service providers must limit access to their facilities and information systems to authorized users and devices and further limit the access of authorized users to only the information and functions that are necessary for their position (WorkSource Policy 1026 – Safeguarding PII). Specific controls include:

   i. **Physical access to service provider facilities** – Due to the confidential and sensitive nature of data being stored and accessed by service provider staff, physical access to this data must be controlled as described below:

      1. All staff with access to confidential data must be provided with a method to secure equipment and hard copies of data containing confidential data, either through a locking office or a secure locking cabinet that cannot be easily removed from the facility.
      2. Any confidential data being viewed by staff during normal business hours must be viewed in a way that unauthorized users cannot inadvertently view the data.
      3. Equipment or hard copies containing confidential data must not be left unattended for any length of time, unless behind a secure lock and out of view. For example, a device can be secured by locking the device in an office or within a locking cabinet.
      4. Access to workstations, servers, and network equipment must be restricted to appropriate staff.
      5. Staff must not access or store confidential data on personally owned employee devices or other devices not managed by the service provider's IT services.

   ii. **Access to physical records or media** – Access to data stored on physical media, such as optical discs (CD/DVD) or universal serial bus (USB) flash drives, as well as paper documents, must be restricted to authorized personnel based on the sensitivity and confidentiality of the data. Access to physical media or paper records containing confidential data must be restricted by a key or combination lock. Employees with access to such data must not share keys or combination values with other employees who are not authorized to access the data.

   iii. **Remote access** – Remote access to a service provider network must utilize a virtual private network (VPN). Any VPN software utilized by service providers must encrypt all remote access traffic based on FIPS 140-2 encryption standards. When accessing a service provider's network or another data system from an external location, staff must mitigate any potential risks identified within this policy. At a minimum, remotely accessing a network must meet the following requirements:

      1. Any remote access of a service provider's network or other data systems must be done so on a trusted network, as defined in Section 2 above. Remote access from untrusted networks, such as public hotspots, or dial-up connections, is not allowed.
      2. When accessing a service provider network remotely, staff must do so using devices and VPN software approved by the service provider.

   iv. **Portable devices** – Portable devices, such as laptops, tablets, and smartphones, must be configured to adhere to the security requirements of this policy and to the following protections:

      1. Devices must be manually locked whenever they are left unattended.

2. Devices must be set to automatically lock after a period of inactivity of no more than 20 minutes.
3. Devices must be kept in a secure area when not in use and when transporting devices outside of a secure area, they must remain under the physical control of an authorized service provider staff person.
4. For portable devices shared by multiple staff, a check-in/check-out procedure is required.
5. For personal mobile devices such as smartphones, remote access to service provider networks is prohibited, with the exception of e-mail clients. Confidential data contained within e-mails may not be viewed on a mobile device.

v. **Installing software on a workstation or portable device** – Automated network security protocols must prevent any unauthorized installations of software on a service provider's internal network.

vi. **Removal of equipment or hard copies from facilities** – Removal of any equipment or hard copies of data containing confidential data from offices, workstations, or remote work locations designated by the service provided is prohibited.

c. **Data storage and transmission** – Storage and transmission of data must follow the internal controls listed below (WorkSource Policy 1026 – Safeguarding PII).

i. **Electronic data storage** – All electronic data created or obtained by a service provider must be stored securely on its internal network or within an external system that meets the security requirements of this policy. Access to data stored on a network that is considered confidential must be restricted to those employees who need it in their official capacity to perform duties in connection with that data. Sharing confidential electronic data owned or obtained by the service provider must only be done so with individuals authorized to access the data.

ii. **Physical data storage** – Confidential data that is stored on physical media, such as optical discs (CD/DVD; Blu-ray) or universal serial bus (USB) drives, must only be accessed on service provider-approved equipment and must be stored in a secure area when not in use. Hard copy documents containing confidential data must be stored in a secure area only accessible to authorized personnel. Sharing confidential physical data owned or obtained by the service provider must only be done so with individuals authorized to access the data.

iii. **Storage requirements for category 4 confidential data** – Any confidential data under category 4 must be identified and stored separately from other types of data and be restricted to only those employees who need it in their official capacity to perform duties in connection with that data. If category 4 data is being stored electronically, the document itself or the folder it is stored in must be password protected.

iv. **Encryption requirements** – Any confidential data owned or obtained by a service provider that is transmitted electronically via e-mail or other methods must be encrypted during transmission.

d. **Return, reuse, and disposal** – All equipment containing data and hard copies containing data owned by a service provider are subject to return, reuse, and disposal requirements. Equipment containing data system media includes, but is not limited to, scanners, copiers, printers, notebook or laptop computers, workstations, servers, network components, and mobile devices (ESD WorkSource Policy 1026 – Safeguarding PII).

i. **Return of assets** – When equipment or paper hard copies are returned from an employee's possession, they are subject to reuse or disposal, as described under Equipment reuse and equipment disposal below. The following requirements apply for returning assets:

1. Any equipment no longer in use must be returned for reuse or disposal.
2. If a staff person is no longer in need of equipment and/or hard copies of data in their possession for their official job duties, this equipment must be returned to the service provider for reuse or disposal.
3. If a staff person leaves employment, the service provider must obtain these items for reuse or disposal.

ii. **Equipment reuse** – Equipment may be reused by service provider staff after clearing or purging any confidential data contained on the device. Additionally, equipment containing data obtained or created by the service provider may be transferred to other service provider agencies and reused after being sanitized by an industry-standard data sanitation method, such as Secure Erase, Random Data, or Write Zero.

iii. **Equipment disposal** – Disposal of any equipment that contains data obtained or created by the service provider must include a sanitation process that removes data from the media in a way that such data cannot be retrieved or reconstructed.

1. **Disposal of storage devices containing only category 1 or category 2 data** – Equipment that includes data containing only category 1 or category 2 data, may be disposed of or recycled after clearing or purging the data contained on the device.
2. **Disposal of storage devices containing category 3 or category 4 confidential data** – Portable hard drives or hard drives in equipment such as notebook or laptop computers, workstations, servers, or mobile devices, that include data containing confidential data, must be disposed of by one of the following methods:
    a. Sanitization by an industry-standard data sanitation method, such as Secure Erase, Random Data, or Write Zero, that ensures data cannot be retrieved or reconstructed; or
    b. Physical destruction of the device that prevents operation or reconstruction.
3. **Disposal of peripheral devices with flash memory** – Printers, scanners, multi-function copier devices, and network components with flash memory storage must have the memory storage cleared before disposal.

iv. **Hard copy disposal** – All hard copies of paper containing confidential data are subject to disposal requirements. Disposal of any hard copies must include a sanitation process that prevents the media from identifying protected data or from being understood or interpreted (such as shredding).

e. **Security awareness** (ESD WorkSource Policy 1026 – Safeguarding PII)

i. **Notification of access to confidential data** –

1. Service provider employees who have access, or are expected to have access in the future, to sensitive, confidential, proprietary, or private data, must be advised of the following:
    a. The confidential nature of the data,
    b. The safeguards required to protect the data,
    c. The expectation that the employee only access or store data that is necessary for their official duties, and
    d. There are civil and criminal sanctions for noncompliance that are contained in the Privacy Act of 1974 and other Federal and state laws.
2. Employees, before being granted access to confidential data, must acknowledge their understanding of the confidential nature of the data and the safeguards with which they must comply as well as the fact that they may be liable to civil and criminal sanctions for improper disclosure.

ii. **Security awareness training** – All service provider staff must receive security awareness training upon hire and annually. New hire training must include the risks of data compromise, an employee's role in prevention, and how to respond in the event of an incident.

f. **Security requirements when working with contractors or partners**

i. The service provider will only share data with organizations who have an active grant or contract with the service provider, for whom the service provider is a grantee, or where a valid data sharing agreement exists between all parties.

ii. Only data necessary for the purposes of carrying out a grant or contract will be shared with grantors, grantees, contractors, or partners.

iii. All data created or obtained by a service provider for the purposes of carrying out a grant or contract awarded by the SWC must be stored securely within a system that meets the security requirements of this policy. Data stored on a shared network that is considered confidential and that may not be accessed by any user who isn't explicitly authorized to access it, must be stored in a secure fashion by password protecting the document containing the data. Sharing data owned by the subrecipient or obtained from the SWC must only be done so with individuals authorized to access the data.

g. **Data security compliance audit** – Data security compliance audits are necessary to ensure security controls are effective and adequate. Audits will identify weaknesses in security controls so that they may be mitigated (ESD WorkSource Policy 1026 – Safeguarding PII).

i. **Audit records** – The service provider must ensure that all information systems create, protect, and retain audit records that can be traced to a specific user, if necessary, to the extent needed to conduct a data security compliance audit or report unlawful or unauthorized activity.

ii. **Auditor requirements** – The service provider may hire an independent auditor or conduct the audit themselves provided they have staff with the skills and experience necessary to perform the audit.

iii. **Audit frequency** – Data security audits must be conducted once every three years to review and assess the effectiveness of existing security controls. Additional audits may be necessary when new IT systems are introduced or existing IT systems are modified, security controls change, or a breach or potential breach is discovered.

iv. **Audit requirements**

1. Data security audits must identify a sampling of IT systems, applications, IT infrastructure, and security controls to test. To the extent possible, an audit must identify a different sampling than the previous audit conducted.
2. Service provider staff must permit the auditor to make onsite inspections during regular business hours for the purpose of conducting audits and/or conducting other investigations to assure compliance with the security requirements of this policy;
3. Any weaknesses identified during the audit must be corrected as soon as appropriate controls can be adequately implemented. The service provider must develop and implement a plan of action to correct any deficiencies identified, if present.
4. Review of user access to data systems to ensure only authorized users have access to them.
5. Review of requisite patches and hotfixes.
6. Inventory of any shared devices.

h. **Security breaches**

i. **Response** – In the event of unauthorized data acquisition that compromises the security, confidentiality, or integrity of confidential data maintained by the service provider, the service provider must respond as follows:

1. A service provider who discovers or is otherwise notified of a security breach will immediately inform the SWC;
2. A risk assessment must be conducted by the service provider immediately following discovery of the data breach in order to identify the root cause(s). Results of the risk assessment will be used to strengthen security protocols to ensure future data breaches do not occur.

ii. **Required notification**

1. **Owner of data** – As required under RCW 19.255.010, in the event of a security breach where any personal data was, or is reasonably believed to have been, acquired by an unauthorized person and the personal data was not secured, the service provider shall notify the owner of the data of this breach of the system immediately following discovery. This notification must be made in the most expedient time possible, without unreasonable delay, and no more than thirty calendar days after the breach was discovered. Notification may be delayed if necessary for the service provider to determine the scope of the breach and restore the reasonable integrity of the data system or if the service provider or the SWC contacts a law enforcement agency after discovery of a breach and a law enforcement agency determines that the notification will impede a criminal investigation. Notice may be provided by written or electronic notice. Electronic notice must be consistent with provisions regarding electronic records and signatures set forth in 15 U.S.C. Sec 7001. Both written and electronic notices must meet the following requirements:
    a. Written in plain language;
    b. Identify the service provider as the reporting agency and include contact information;
    c. Include a list of the types of personal information that were or are reasonably believed to have been the subject of the breach;
    d. Include a time frame of exposure, if known, including the date of the breach and the date of the discovery of the breach; and
    e. Include toll-free telephone numbers and addresses of major credit reporting agencies.

2. **Department of Labor – Employment and Training Administration (ETA)** – As required in TEGL 39-11, any breach or suspected breach of confidential personal data associated with an ETA funded grant must immediately be reported to the Federal Project Officer responsible for the grant and to ETA Information Security at ETA.CSIRT@dol.gov, (202) 693-3444, and follow any instructions received from officials of the Department of Labor.
3. **Employment Security Department (ESD)** – As required in Washington State WorkSource Policy 1026 – Safeguarding Personally Identifiable Information (PII), any breach or suspected breach of PII must immediately be reported to the Employment Security Department (ESD) at SystemPolicy@esd.wa.gov using "PII Incident" in the subject line. For grants managed by ESD, such as WIOA Title III, service providers must also follow ESD HR Policy 0031-1. This notification must include the following content:
    a. Workforce Development Area (WDA)
    b. Reporting Entity-LWDB, subrecipient, contractor, other and contact information
    c. Date of Incident
    d. Date of Discovery (if different)
    e. Number of files breached or affected
    f. Type of Issue:
        i. Hard copy files or information
        ii. Electronic files or information
    g. Description of the incident
    h. Initial Determination of level of incident:
        i. Carelessness
        ii. Negligence
        iii. Fraud
        iv. Theft
        v. Other
    i. Any other relevant information
    j. If staff member is also an ESD employee, please refer to ESD HR Policy 0031-1-Security Breach Notification;
    k. If a Social Security Administration (SSA) related data breach/security incident, include "SSA" in the title;
    l. If ESD equipment loss or theft is involved, ESD staff must complete a Security Incident Report

i. **Security violations** – Service provider staff who violate the provisions within this policy or associated procedures must receive corrective action to a degree appropriate for the severity of the violation.
    i. **Investigation** – When a violation is discovered, either through a security compliance audit or self-reported, the service provider will notify the SWC within 24 hours that an investigation is commencing. The service provider must consider the following items and make a determination to be brought to the SWC within 30 days of the incident for review and determination of next steps:
        1. The nature and severity of the violation and its impact as determined by the security audit in section 3.c.i. above;
        2. Whether or not this is a first or repeat violation;
        3. Whether or not the employee involved was properly trained;
        4. Relevant legislation or contract provisions;
        5. Whether or not the employee involved has cooperated with federal, state, or local investigators or the SWC.
    ii. **Security violation categories** – Based on review of the investigation items above, the SWC will categorize a violation as follows:
        1. **Category 1 violation** – Actions which violate federal, state, or local laws and regulations, including but not limited to:

a. Improper disclosure of protected health information, personal information that violates federal or state privacy laws, or that violates Washington state identity theft protection law;

b. Use of data to threaten, harass, or intimidate others;

c. Use of data or information systems to engage in any other illegal activities.

2. **Category 2 violation** – Actions that violate this policy or associated procedures, but do not otherwise violate federal, state, or local laws and regulations, include but are not limited to:

a. Improper or excessive use of service provider data or information systems for non-business purposes, such as excessive use of e-mail or internet access for personal use or visiting potentially harmful websites;

b. Unauthorized attempts to bypass service provider data security controls, such as disabling antimalware software or firewalls, giving other employees your username/password combination, or preventing software patching beyond the allowed timeframe;

c. Inappropriate viewing, displaying, or storing of materials that are commonly seen as offensive or threatening, or that contains sexually explicit or obscene language or content, or contains any content prohibited by the service provider's harassment policy.

iii. **Corrective action guidelines** – A sanction for a violation will be applied by the service provider based on the category that the violation has been assigned and are defined as follows:

1. **Category 1 corrective actions** – Incidents in this category may require notification of appropriate law enforcement agencies, government regulatory agencies, and any individuals affected. Sanctions that may be applied from this category include:

a. Revocation of access to the service provider's network or other data systems involved;

b. Requirement that the employee undergo additional training on security and privacy practices;

c. Disciplinary action or termination of employment.

2. **Category 2 corrective actions** – Actions that may be applied from this category include:

a. A warning that a portion of this policy or associated procedure was violated;

b. A requirement that the employee undergo additional training on security and privacy practices;

c. Revocation of access to the service provider's network or other data systems involved;

d. Disciplinary action or termination of employment.

4. Action Required

This policy must be communicated to all service provider staff. Service providers must have the requirements of this policy implemented within 120 days of publication.

5. References

- Washington WorkSource Policy 1026 – Safeguarding Personally Identifiable Information (PII)
- Office of the Chief Information Officer (OCIO) Policy 141.10
- TEGL 39-11 – Guidance on Handling and Protection of PII
- RCW 19.255.010 – Notice of security breaches

6. Supersedes

N/A

Revision History:
N/A