DATA PRIVACY (PII) AND SECURITY REQUIREMENTS POLICY #2010 Rev 3

Date of Original Policy: 12/09/2020
Effective Revision Date: 5/19/2026

PURPOSE

This policy describes WSW data security requirements to ensure privacy of all protected and confidential records. Including, the requirements for safeguarding participant's personally identifiable information (PII) that align with federal Workforce Innovation and Opportunity Act (WIOA) law, regulation, and guidance.

BACKGROUND

It is necessary to periodically collect personally identifiable information (PII) in order to verify, document, and enroll eligible customers into WIOA Title I and Wagner-Peyser Act programs 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. Therefore, it is imperative that proactive methods are implemented to ensure this critical, sensitive, personal information is protected at all times. WSW Subrecipients must have written internal controls for safeguarding PII following ESD Policy #1026 Rev 1.

POLICY

The majority of WSW's confidential information is in the form of reporting and data collected from multiple Management Information Systems. WSW does not provide direct services to customers therefore it is highly unlikely WSW staff will collect confidential information. Except in certain approved situations in which case safeguards will be put in place.

1. **Data classification:** a category of information 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:
    - **A. 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.
    - **B. 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 WSW, 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.
    - **C. 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:
        - i. **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:

1. Social security number
2. Driver’s license number or Washington identification card number
3. Account number, credit or debit card number, 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
4. Home telephone number
5. Age
6. Full date of birth
7. Marital status
8. Spouse’s name
9. Educational history
10. 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
11. Financial information
12. Computer password
13. Any information, that when combined with other personal or identifying information, is linkable to a specific individual, including but not limited to:
    a. First name (or first initial) and last name
    b. Student, military, or passport identification number
    c. Health insurance policy number or health insurance identification number
    d. Username or email address in combination with a password or security questions and answers that would permit access to an online account
    e. Business address
    f. Business telephone number
    g. General education credentials
    h. Gender
    i. Race

ii. **Lists of individuals for commercial purposes:** though first name (or first initial) and last name are not confidential by themselves, lists of individuals by name must be protected from release or disclosure for commercial purposes (RCW 42.56.070 (8)).

iii. **Network infrastructure and security information:** information regarding the infrastructure and security of computer and telecommunications networks owned or utilized by the WSW 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 (RCW 42.56.420 (4)).

D. 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:

i. Any information about an individual's medical history or 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.

ii. 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.

2. **Configuration and security controls** – WSW limits access to its facilities and information systems to authorized users and devices and further limits the access of authorized users to only the information and functions that are necessary for their position.

   WSW staff will have limited access, with assigned permissions, to certain user/program shared folders depending on their assigned duties. Annual review of user groups is facilitated by WSW Chief Operating Officer and managed IT service provider. If a WSW staff person quits or is terminated, WSW Operations Manager informs the WSW managed IT service provider to deactivate their access to all data systems and network on their last day of work.

   Specific controls include:

   A. System Protection – All equipment is monitored by WSW's managed IT provider who ensures:

      i. All security patches and hotfixes are applied quarterly or earlier as needed and

      ii. All workstations and laptops have Anti-Malware application installed and updated.

   B. Physical access to WSW facilities – due to the confidential and sensitive nature of information being stored and accessed by WSW staff, physical access to WSW facilities is controlled as described below:

      i. All WSW staff with access to confidential data are provided with secure equipment and/or hard copies of information containing confidential data, either through a locking office or a secure locking cabinet that cannot be easily removed from the facility.

      ii. Any confidential information being viewed by WSW staff during normal business hours must be viewed in a way that unauthorized users cannot inadvertently view the information.

      iii. Equipment or hard copies containing category 3 or category 4 information 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.

      iv. Access to WSW's servers and network equipment is restricted to the WSW Office Manager, Chief Operating Officer, and the WSW's managed IT provider.

   C. Access to WSW network and information systems – only devices approved by the WSW's Chief Operating Officer are authorized to access the WSW's internal network or an information system necessary for WSW operations. Authorized users must have permissions granted through IT managed service provider.

   D. 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 information must not share keys or combination values with other employees.

Access to stored electronic records containing confidential information is limited to authorized personnel only. Records are purged according to record retention requirements for that specific funding. Electronic records can only be transmitted through an approved encrypted email channel or uploaded to an approved secure site protected by passwords.

E. User account authorization and authentication

i. **Information security roles and responsibilities** – the WSW has two security roles for its internal network, which are described below. Users in either role must ensure that only the employee to whom the account is assigned knows the account logon ID and password combination. Security roles for systems not owned by the WSW, but necessary for WSW operations, are defined within the documentation for the system in question.

1. **Staff** – provides general access to the WSW's network. Software installation or removal and access to system settings is restricted.
2. **Administrator** – provides administrative access to the WSW's network. Software installation or removal and access to system settings is unrestricted.

ii. **Authentication, password creation, and password aging requirements**

1. **Authentication** – the WSW utilizes the DUO authentication protocol for multifactor authentication to access the network and sensitive systems. Once authenticated into the system data transfers protocols utilize advanced encryption standard (AES) required for Federal information processing standards. Only users authenticated through this process can access data on the WSW network. Failed logon attempts will lock a user's account for a full 10 minutes after 10 failed attempts
2. **Password creation and aging requirements –** creating or changing a password on the WSW network is enforced by industry standard complex password requirements and must be changed every 180 days. The complex password requirements are as follows:

- Must not contain any part of staff's name
- Must be at least 10 characters in length
- Must include characters from at least 3 of the 4 categories
- Uppercase characters A-Z (Latin alphabet)
- Lowercase characters a-z (Latin alphabet)
- Digits 0-9.
- Special characters (!, $, #, %, etc.)

When changing a password, it must be significantly different from previous four versions of passwords. For instance, changing a number within the password incrementally is not sufficiently different to meet this requirement. Sharing of passwords is prohibited.

3. **Remote access** – the WSW allows for remote access to its network through Office 365 One Drive authorized users only.

Remote access to other data systems can be used when allowed by those systems. When accessing the WSW 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:

a. Any remote access of the WSW network or other data systems necessary for WSW operations must be done so on a trusted network. Remote access from untrusted networks, such as public hotspots in airports or hotels, or dial-up connections, are not allowed.

b. When accessing the WSW network remotely, WSW staff must do so using WSW approved devices.

F. Portable devices – all WSW staff utilize portable devices, such as laptops, tablets, and smartphones, for their day-to-day work and to access the WSW network. These devices are configured to adhere to the security requirements of this policy. Staff utilizing these devices must adhere to the following protections:

i. Manually lock devices whenever they are left unattended.

ii. Ensure devices are set to automatically lock after a period of inactivity of no more than 20 minutes.

iii. Keep devices in a secure area when not in use and when transporting devices outside of a secure area, ensure they are under the physical control of authorized WSW staff at all times.

iv. For devices shared by multiple staff, a check-in/check-out procedure is required.

v. Protected data should not be downloaded or saved to computer hard drive; printed; emailed (unless encrypted and sent to other authorized users only); or saved on physical media.

G. Installing software on a workstation or portable device – automated network security protocols prevent any unauthorized installations of software on the WSW's internal network. Employees who have a valid business need for, and who wish to install software on their workstation or portable device, must first obtain approval from the WSW's Chief Operating Officer before installing the software. Only employees with the administrator security role, or the WSW's managed IT provider, may install software on a workstation or portable device.

H. Backup Cloud Storage – WSW's IT provider manages the frequent back up of all data stored on the network. This ensures consistent scheduling and the ability for a quick response in case of a disaster. Data is encrypted at all times. If backup is needed to restore data, the data will be placed back on the network by the IT provider. It will not be downloaded to individual workstations or portable devices.

I. Purging of Data – WSW will follow WSW Records Retention Policy 2002 for retention limits for specific grant documents. When purging/disposing of PII, WSW will shred all paper documents using an outside secure company. For electronic files they will be removed from all active and inactive storage. Using WSW Managed IT provider if necessary to ensure complete, secure removable of the files. If PII is located on the State MIS, the purging/disposing of that information is the responsibility of the State. If PII is located on a WSW owned CRM, the information will remain in the CRM until or unless CRM becomes obsolete at which point the CRM Vendor and IT Provider will work together to properly dispose or archive the information for the required retention period.

3. Security awareness

A. **Acceptable uses of computer systems and user responsibilities** –

i. **Acceptable use of data** – any data owned or obtained by the WSW may only be used for official business of the WSW.

ii. **Acceptable use of software** – usage of software by WSW staff must be used in accordance with the software's terms of service and applicable licensing and copyright laws.

iii. **Accessing confidential data** –all category 3 and category 4 data owned or obtained by the WSW must be accessed using WSW-issued equipment, using WSW managed information technology (IT) services, and in designated locations approved by the WSW. Confidential information that is accessed must not be left open and unattended. Accessing category 3 or category 4 data on personally-owned equipment (including portable and mobile devices), at off-site locations such as the employee's home, and using IT services not managed by the WSW such as Gmail, is strictly prohibited unless approved in writing by WSW Chief Executive Officer or WSW Chief Operating Officer. The WSW has approved the following locations for accessing confidential data:

1. Workforce Southwest Washington – 805 Broadway, Suite 412, Vancouver, WA 98660
2. Next – 2901 E Mill Plain Blvd, Vancouver, WA 98661
3. WSW staff work remotely from their homes. Therefore, working from home is approved and accessing confidential data digitally is also approved.
4. Any location in the state of Washington managed by the Employment Security Department (ESD) or a State or Local Workforce Development Board.

B. **Notification and Training to access confidential information** –

i. WSW employees who will have access to or are expected to have access to in the future, sensitive, confidential, proprietary, or private data will be advised of the confidential nature of the information. Employees must be aware of and follow the Privacy Act of 1974. Any unauthorized access of confidential information, unauthorized disclosure of such data, negligence or carelessness in use of such data may result in correction action, appropriate sanctions, dismissal from employment, or potential criminal penalties under the Privacy Act of 1974. This information will be provided by WSW annually during the Privacy and Security Awareness Training with an opportunity for additional technical assistance.

ii. Employees, before being granted access to confidential information, 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. Staff will sign the form that is appropriate for the data they will access.

C. **Non-Compliance** – if for any reason WSW staff are in noncompliance with this policy, their access to secure folders and files will be revoked and/or disciplinary action taken.

i. If data was compromised or potentially compromised from a specific program. WSW will notify program contact within one (1) business day of discovery.

ii. WSW Chief Operating officer will also take action to mitigate risk of loss.

4. **Breach**

A. **Reporting** –

i. Any WSW employee that becomes aware of a breach of security, any release of information, loss, theft, or suspected authorized access of PII must immediately (within 12 hours) submit the following to WSW Chief Operating Officer:

1. Name of reporting representative
2. Date of Incident
3. Date of Discovery (if different from above)
4. Number of files breached or affected
    a. Type of Issue – Hard Copy Files or Electronic/Digital
5. Description of the Incident
6. Initial Determination of Level of Incident:
    a. Carelessness
    b. Negligence
    c. Fraud
    d. Theft
    e. Other – please provide specifics
7. Any other relevant information

ii. Process for reporting a breach or suspected breach will be written in Subrecipient or Subcontractor's contract with WSW.

B. WSW Response –

i. WSW will immediately notify ESD in accordance with Policy 1026 Rev 1.

ii. If the suspected breach is from a WSW, Subrecipient, or partner owned equipment or office, WSW will immediately begin an investigation.

1. Document investigation with the facts, including if local internal controls and policies were followed.
2. Notify Director or Manager of a corrective action or dismissal from employment is necessary.
3. Notify additional entities if breach affected their system, customer, or business process. Confirm corrective action or dismissal of employee.
4. Issue a closure document to all parties involved including individual(s) affected once steps are completed and breach is resolved.

5. Monitoring – WSW will evaluate and monitor PII compliance with statutes, regulations, and terms of awards annually. This will occur for WSW Subrecipients and Subcontractors during their scheduled annual program monitoring and for internal WSW Employees during annual training.

Any corrections to the WSW internal process or procedures will be documented during the annual evaluation.

DEFINITIONS

- **Breach:**

Security – unauthorized acquisition of unsecured data, account credentials, encryption keys or other means used to decipher secured information that is maintained by the WSW.

- Data – actual or suspected compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access and/or any similar occurrence where:
  1. An unauthorized user accesses or potentially accesses PII, or
  2. An authorized user accesses or potentially accesses PII for unauthorized purposes.

- **Trusted network:** a network that includes security controls. At a minimum, these controls must include a firewall, 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.
- **Security incident – A set of events that have been examined and determined to indicate a violation of security policy or an adverse effect on the security status of one or more systems within an organization or entity.**

REFERENCES

- ESD Policy Safeguarding Personally Identifiable Information (PII) #1026 Rev 1
- Training and Employment Guidance Letter (TEGL) 39-11
- 20 CFR 683.220
- 2 CFR 200.303
- Guidance on the Protection of Personal Identifiable Information I U.S. Department of Labor (dol.gov)
- RCW 19.255
- WSW Records Retention Policy #2002 Rev 3

SUPERSEDES

- WSW Data Privacy and Security Requirements Policy #2010 effective date 12/09/2020
- WSW Data Privacy (PII) & Security Requirements Policy #2010 Rev 1 effective date 03/12/2024
- WSW Data Privacy (PII) & Security Requirements Policy #2010 Rev 2 effective date 01/28/2026

WEBSITE

http://workforcesw.org/providers#OperationsPolicies

INQUIRIES

Please contact Amy Gimlin agimlin@workforcesw.org (360) 567-1059 for questions.