# DATA PRIVACY AND SECURITY REQUIREMENTS POLICY #2010:

Date of Original Policy: 12/09/2020

## PURPOSE:

This policy describes WSW data security requirements to ensure privacy of all protected and confidential records.

## BACKGROUND:

WSW from time to time comes in contact with Personal Identifiable Information (PII) and other confidential information related to workforce programs. According to regulations, access must be restricted and monitored.

## POLICY:

**A. 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 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 Chief Operating Officer 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:

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

1. All security patches and hotfixes are applied quarterly or earlier as needed and
2. All workstations and laptops have Anti-Malware application installed and updated.

ii. **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:

1. 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.
2. 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.
3. 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.

4. 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.

iii. **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. WSW physical server is in a locked room within the WSW offices. Access to the key is limited to WSW Office Manager and WSW Chief Operating Officer.

iv. **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.

v. **User account authorization and authentication**

1. **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.

   a. **Staff** – provides general access to the WSW's network. Software installation or removal and access to system settings is restricted.

   b. **Administrator** – provides administrative access to the WSW's network. Software installation or removal and access to system settings is unrestricted.

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

   a. **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

   b. **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 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.

3. **Remote access** – the WSW allows for remote access to its network through VPN. VPN software is setup for staff by the WSW's managed IT provider in coordination with the WSW's Chief Operating Officer. VPN software utilized by the WSW is NIST validated and encrypts all remote access traffic based on FIPS

140-2 encryption standards. 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 and VPN software.

vi. **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:

a. Manually lock devices whenever they are left unattended.

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

c. 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.

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

e. 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.

f. For mobile devices such as smartphones, remote access to the WSW network is prohibited.

vii. **Installing software on a workstation or portable device** – automated network security protocols prevents 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.

viii. **Backup Cloud Storage** – WSW's IT provider manages the frequent back up of all data stored on the network. This ensures consistent scheduling and 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.

**B. Security awareness**

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

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

2. **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.

3. **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 the CEO or WSW Chief Operating Officer. The WSW has approved the following locations for accessing confidential data:

a. Workforce Southwest Washington – 805 Broadway, Suite 412, Vancouver, WA 98660
b. Next – 120 NE 136th Avenue # 130, Vancouver, WA 98684
c. Longview Goodwill – 1030 15th Avenue, Longview, WA 98632
d. During the COVID pandemic, all WSW staff are working remotely from their homes. Therefore, as long as working from home is approved accessing confidential data digitally is also approved.
e. Any location in the state of Washington managed by the Employment Security Department (ESD) or a State or Local Workforce Development Board.

ii. **Notification of access to confidential information** –

1. WSW employees who will have access to, or are expected to have access to in the future, sensitive, confidential, proprietary, or private data must be advised of the confidential nature of the information, the safeguards required to protect the information, and that there are civil and criminal sanctions for noncompliance with such safeguards that are contained in Federal and state laws.
2. 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.

iii. **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.

1. If data was compromised or potentially compromised from a specific program. WSW will notify program contact within one (1) business day of discovery.
2. WSW Chief Operating officer will also take action to mitigate risk of loss.

## DEFINITIONS:

- **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:
  - **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 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.
  - **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:

- Social security number
- Driver's license number or Washington identification card number
- 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
- Home telephone number
- Age
- Full date of birth
- Marital status
- Spouse's name
- 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
- Computer password
- Any information, that when combined with other personal or identifying information, is linkable to a specific individual, including but not limited to:
  - First name (or first initial) and last name
  - Student, military, or passport identification number
  - Health insurance policy number or health insurance identification number
  - Username or email address in combination with a password or security questions and answers that would permit access to an online account
  - Business address
  - Business telephone number
  - General education credentials
  - Gender
  - Race

- **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)).
- **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)).

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

**WEBSITE:**

http://workforcesw.org/providers#OperationsPolicies

**INQUIRIES:**

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