WSW Joint Executive/Finance Committee Meeting
Zoom Conference Call
January 24, 2024 3:30 – 5:00 pm
AGENDA

3:30	Welcome	**A.D. Simmons**
3:35	Consent Agenda • Minutes, Contract & Policy Memos *	**A.D. Simmons**
3:40	Finance • Audit Report *	**Barri Blair** **Craig Catlin & Athalia Bowrey – Johnson, Stone & Pagano, P.S.**
4:20	CEO Update • Bylaw Attendance Updates • Strategic Planning • EcSA State Funding Update • Spring Board Retreat – May 29, 2024	**Miriam Halliday**
4:55	Open Discussion / Other Items	**A.D. Simmons**
5:00	Adjourn	**A.D. Simmons**

*** - Action Required**

NOTES

February 28, 2024 – Executive Committee Meeting - Zoom
March 27, 2024 – Executive Committee Meeting - TBD

WSW Executive/Finance Committee Meeting Minutes
December 5, 2023
3:30 p.m.
Hybrid

Executive Committee Members Present: A.D. Simmons (via Zoom), Corey Giles (via Zoom), Adrienne Watson (via Zoom), Monte Constable, Renny Christopher (via Zoom), and Ted Sprague (via Zoom).

Finance Committee Members Present: Renny Christopher (via Zoom), Ilona Kerby (via Zoom), Jim Lucey (via Zoom), and Bob Gustainis (via Zoom).

Executive/Finance Committee Members Not Present: Paige Spratt, John Vanderkin, Sue Marshall, and Mark Tishenko.

Staff Members Present: CEO Miriam Halliday, Amy Gimlin, Barri Blair, and Traci Williams.

WELCOME:
Vice Chair A.D. Simmons opened the meeting at 3:34 p.m. and welcomed everyone in attendance.

APPROVALS:
Having reached quorum, Vice Chair Simmons entertained a motion to approve the Consent Agenda, consisting of the Executive Committee minutes held on October 25,2023, Contract Memo, and Policy Memo containing; WSW Supportive Service Policy #3005-10, WSW Training Policy Handbook – Attachment A, WSW Youth Incentives Policy #3042.

Renny Christopher moved to approve the Consent Agenda as presented, second by Bob Gustainis. Motion carried.

FINANCE:
Treasurer Renny Christopher entertained a motion to approve the Finance Committee minutes held on August 16, 2o23.

Ilona Kerby moved to approve the Finance Committee minutes as presented, second by Jim Lucey. Motion carried.

CFO, Barri Blair presented the highlights of the revised WSW PY23 annual budget. CFO Blair presented all the revisions that were made as noted on the budget memo for the PY23 budget revision. Questions and comments were invited and answered by CFO Blair.

Ilona Kerby moved to approve the recommendation of the budget revision to the full board for final approval at the December board meeting as presented, second by Adrienne Watson. Motion carried.

BOARD BUSINESS:

- **Board Member Nomination**

Governance Chair, A.D. Simmons gave a brief overview of the new potential board member, Corie Dow-Kramer, Executive Director for Youth and Family Link under Community-Based Organization. The Governance Committee and CEO Halliday recommends that Corie Dow-Kramer be put forward to the full board for nomination. A motion was entertained to approve Corie Dow-Kramer to the full board at the December 12th meeting.

Renny Christopher moved to approve Corie Dow-Kramer to the December 12th board meeting for final approval, second by Ted Sprague. Motion carried.

CEO UPDATE:

CEO Halliday went over the upcoming December board agenda draft and shared with the Executive Board how the November WWA conference went. CEO Halliday gave updates around the Economic Security for All – State funding and what to expect in the coming year. Also touched on was the Strategic Planning that WSW and the full board will be focusing on at the December board meeting and throughout the first part of 2024. CEO Halliday brought to the Executive board an opportunity to give the WSW team December 26-29th off as Holiday PTO days for all the hard work the team has put in.

Adrienne Watson moved to approve December 26-29th as holiday PTO days to the full WSW Team, second by Ted Sprague. Motion carried.

NEW BUSINESS / OTHER ITEMS

None was forthcoming.

ADJOURNMENT:

With nothing further for the good of the order, Vice Chair Simmons entertained a motion to adjourn the meeting at 4:11 p.m.

workforce
SOUTHWEST WASHINGTON

CONTRACT MEMO

DATE: JANUARY 18, 2024

TO: MIRIAM HALLIDAY, WSW CHIEF EXECUTIVE OFFICER

WSW EXECUTIVE BOARD MEMBERS

FROM: LINDA CZECH, WSW CONTRACTS MANAGER

RE: CONTRACT UPDATE (DEC-JAN 2024)

WSW ***modified*** the following contracts:

- Wahkiakum Health and Human Services to reduce budget by $27,000 for total budget amount **$63,000,** no change in end date of **June 30, 2024**.
- Career Path Services to increase budget by $1900 for total budget amount **$450,320**, no change in end date of **September 30, 2024**.
- Nancy Pionk Coaching and Consulting to extend contract to **June 30, 2024**.

WSW ***notification of grant award/execution***:

- WSW received a grant award for Economic Security for All (EcSA) Community Reinvestment Funds from Employment Security for **$1,762,986,** end date **May 31, 2025**.
- WSW received a grant modification for Economic Security for All (EcSA) from Employment Security to adjust the indirect rate, no change in amount or end date of **June 30, 2024**.
- WSW received a grant modification for Workforce Innovation and Opportunity Grant from Employment Security to increase PY22 budget by $91,806 total budget of **$3,988,006**.
- WSW received a grant award for Future Leaders Project from Department of Labor for **$350,000**, end date **December 31, 2025**.

workforce
SOUTHWEST WASHINGTON

POLICY MEMO

DATE: JANUARY 18, 2024

TO: MIRIAM HALLIDAY
WSW EXECUTIVE COMMITTEE MEMBERS

FROM: TRACI WILLIAMS, WSW OFFICE MANAGER/EXECUTIVE ADMINISTRATOR

RE: POLICY UPDATES

WSW Stevens Amendment Requirements Policy 2011-1

This was a revision to our Stevens Amendment Requirements Policy. This policy was revised to communicate the requirement that all recipients of U.S. Department of Labor (DOL) grants include the Stevens Amendment funding disclosure language and web links for all state and local projects, programs, or activities that utilize those funds.

Based on the approval process, this policy approval falls under **Tier 3 Executive Committee** and Full Board **approval**.

Tier 3 – Substantial

> Definition: Substantial revisions consist of significant revisions to a current policy or a State or Federal mandated "new" policy with local revisions made that will affect service delivery. These revisions require approval from both the **Executive Committee** and Full Board.

WSW Data Privacy (PII) and Security Requirements Policy 2010-1

This was a revision to our Data Privacy and Security Requirements Policy. This policy was revised to incorporate the requirement that grantees of the U.S. Department of Labor funds have an internal control structure and written policies in place to provide safeguards to protect Personally Identifiable Information (PII). Adding PII to the policy name was also revised.

Based on the approval process, this policy approval falls under **Tier 3 Executive Committee** and Full Board **approval**.

Tier 3 – Substantial

> Definition: Substantial revisions consist of significant revisions to a current policy or a State or Federal mandated "new" policy with local revisions made that will affect service delivery. These revisions require approval from both the **Executive Committee** and Full Board.

WSW THRIVE – State Incentives Policy 3502

This is a new policy for WSW. WSW created this policy to provide guidance to our local service providers on the procedures associated with this new resource through the Department of Commerce, Community Reinvestment Project. Incentives will support the retention and engagement of State Thrive participants as they overcome employment barriers and gain additional education/credential.

Based on the approval process, this policy approval falls under **Tier 3 Executive Committee** and Full Board **approval**.

Tier 3 – Substantial

> Definition: Substantial revisions consist of significant revisions to a current policy or a State or Federal mandated "new" policy with local revisions made that will affect service delivery. These revisions require approval from both the **Executive Committee** and Full Board.

STEVENS AMENDMENT REQUIREMENTS POLICY #2011 Rev 1

Date of Original Policy: 12/21/2021
Effective Revision Date: 3/12/2024

PURPOSE

Workforce Southwest Washington (WSW) has established ~~this a~~ policy to ensure compliance with the Stevens Amendment. WSW integrates State ESD Policy 1027 guidance, in revision 1 of this local policy, to update and ensure funding information language for WSW federally funded projects or programs.

BACKGROUND

WSW has established the following policy pursuant to P.L. 115-141, Division H, Title V, Section 505. P.L. 115-141, Division H, Title V, Section 505 is an appropriations provision that requires grantees of the Departments of Labor (DOL), Health and Human Services (HHS), and Education to disclose for a grant program the percent of the costs financed with federal funds, the federal dollar amount, and the percentage and dollar amount financed by nongovernmental funds. Additionally, a different two-part formulation of the Stevens Amendment is included in the Department of Agriculture's (USDA's) general permanent statutory authority at 7 USC 2209d.

The policy requirements below are separate from those in 2 CFR 200 and, when appropriate, both must be complied with.

POLICY

a. Stevens Amendment Language Content

WSW staff as well as WSW's Subrecipient Program Operators and Managers will include a statement in all applicable outreach and marketing materials acknowledging the use of Federal funds. Applicable outreach and marketing materials include but are not limited to - statements; press releases; requests for proposals; bid solicitations; and other documents (see subsection b., Documents Subject to Disclosure) describing projects or programs funded in whole or in part with Federal money.

All grantees receiving Federal funds, including but not limited to State and local governments and recipients of Federal research grants, shall clearly state:

1. The dollar amount and percentage of Federal funds for the project or program,
2. Federal funding entity (name of the fund allocation, grant, or program),
3. The funding period, and
4. The dollar amount and percentage of non-governmental sources of funds for the project or program,

b. Documents Subject to Disclosure

Under the Stevens Amendment, "documents" is any communication including but not limited to, public statements, social media posts, toolkits, resource guides, websites, and visual presentations. For example, an emailed newsletter intended for the public that describes a federally funded program requires the disclosure statement.

The following list includes some examples of documents or other publications that may describe a project or program that federal money funds in whole or in part:

- Bids for solicitations
- Blogs/vlogs
- Brochures
- E-mail blasts
- Manuals
- Press releases
- Promotional materials (e.g., fliers, posters, advertisements)
- Requests for proposals (e.g., supplemental and continuation proposals)
- Resource guides
- Documents that include statements about the program or project
- Toolkits
- Visual presentations (e.g., PowerPoint presentations)
- Equal Opportunity and Grievance/Compliant handouts provided to enrollees

c. Organizational websites "describing projects or programs," defined as: any communication in furtherance of accomplishing the goals of the federal project or program for which the grantee has an award, are subject to the Stevens Amendment disclosure statement.

For example, an organizational website page that describes DOL programs over which the organization has administrative and/or operational oversight, such as WIOA Title I-B, National Dislocated Worker Grants, etc.

d. Contracts do not require the Stevens Amendment disclosure statement. The disclosure is necessary only when issuing statements, press releases, RFPs, bid solicitations, and other publicly available documents describing projects or programs funded in whole or in part with federal money.

e. The Stevens Amendment is not required on all pages of a document or communication nor is it required on each separate web page. At least one page must contain the disclosure statement.

f. To minimize waste of costly resources, existing printed documents that do not include the Stevens Amendment disclosure need not be thrown away and may continue to be used, but any reprinting, republication of existing documents, or creation of new documents or materials must be updated subsequent to publication of this policy and future printings must meet Stevens Amendment requirements.

i. Allowance of Hyperlinks. When it is not practical to include all elements from 3.a. above within a communication, a hyperlink to the funding information is sufficient, along with the statement:

"This [fill in the blank-project(s)/program(s)] receive(s) support and funding from a U.S. Department of Labor [fill in the blank] grant(s) provided through Workforce Southwest Washington. Read more about WSW federal funding at www.workforcesw.org."

WSW has developed a web page providing funding for the program or fiscal year, which can be found on the linked footer of www.workforcesw.org.

Examples of appropriate compliance statements:

If the document includes all four (4) of the elements in Section 3.a. (above) in the body of the document, no additional Stevens Amendment statement or weblink is needed.

1. Full Stevens Amendment funding statement containing all the elements in section 3.a.

   For Example: "The local WIOA Youth program is supported by the USDOL Employment and Training Administration. $765,123 (93.9% of total) is financed by PY23 allocation of Federal funds to Workforce Southwest Washington, and $50,000 (6.1% of total) is being financed by other sources."

   OR

2. ***"This [fill in the blank-project(s)/program(s)] receive(s) support and funding from a U.S. Department of Labor [fill in the blank] grant(s) provided through Workforce Southwest Washington. Read more about WSW federal funding at WSW Funding Disclosures."***

g. Compliance and Monitoring

WSW, as the Administrative Entity and Fiscal Agent for the Southwest Workforce Area and its subrecipients of WIOA funds, will formally monitor annually, the outreach and marketing materials distributed by self or subrecipients receiving state or federal dollars in accordance with the grant requirements.

REFERENCES~~:~~

- Consolidated Appropriations Act, 2023 specifically Div. H, Title V, Sec. 505
- ESD Policy 1027

WEBSITE

http://workforcesw.org/providers#OperationsPolicies

INQUIRIES

Please contact ~~Amy Gimlin~~Tamara Toles ttoles~~agimlin~~@workforcesw.org (360) 567-105~~759~~ with questions.

DATA PRIVACY (PII) AND SECURITY REQUIREMENTS POLICY #2010 Rev 1

Date of Original Policy: 12/09/2020
Effective Revision Date: 03/12/2024

PURPOSE~~:~~

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

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. ~~Because both direct recipients of federal funds and WSW staff, subrecipients, and contractors may have access to individuals' PII, it is~~ 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. ~~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~~:~~

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.

~~1.~~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 ~~Chief Operating Officer~~Office 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. ~~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.~~ 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.

~~D.~~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 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~~Office 365 One Drive authorized users only. ~~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~~.

~~E.~~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.

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

~~F.~~G. **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.

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.

~~2.~~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 ~~the CEO~~ 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 – 120 NE 136th Avenue # 130, Vancouver, WA 98684
3. Longview Goodwill – 1030 15th Avenue, Longview, WA 98632
4. ~~During the COVID pandemic, all~~ WSW staff ~~are~~ wo~~r~~k~~rking~~ remotely from their homes. Therefore, ~~as long as~~ working from home is approved and accessing confidential data digitally is also approved.
5. 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 ~~of~~ to access ~~to~~ confidential information** –

i. WSW employees who will have access ~~to, or~~to or are expected to have access to in the future, sensitive, confidential, proprietary, or private data ~~must~~ will 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~~. 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 Quality and Compliance Manager 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.

~~ii.~~

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. If the suspected breach is from an ESD owned equipment or office, WSW will immediately notify ESD in accordance with Policy 1026.

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 Quality and Compliance Manager 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~~:~~

~~**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:~~

- **Breach:**
  - ~~o~~ Security – unauthorized ~~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~~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
  ~~1.~~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.

REFERENCES:

- ESD Policy Safeguarding Personally Identifiable Information (PII) #1026
- 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

WEBSITE:

http://workforcesw.org/providers#OperationsPolicies

INQUIRIES:

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

THRIVE – STATE INCENTIVES
POLICY #3502

Date of Original Policy: 03/12/2024

PURPOSE

To provide guidance and procedures to utilize Department of Commerce's (DOC) Community Reinvestment Funds (CRF) in a fair and equitable manner. These incentives are also known as Career Accelerator Incentives in which Subrecipient(s) will issue Incentives for enrolled State Economic Security for All (Thrive) participants, whose household is making satisfactory progress in State Thrive services and activities. The goal for providing the incentive is to retain the participant in Thrive activities and/or cover expenses which may deter retention or successful completion of the training and/or assist in attainment of income adequacy.

BACKGROUND

Thrive is a poverty reduction model that coordinates existing programs to increase their collective ability to support low-income Washingtonians in their pursuit of equity, dignity, and sustained self-sufficiency. In 2022, the Washington State Legislature set aside 200 million dollars to create the Community Reinvestment Account. This fund was designated to address racial, economic, and social disparities created by the historic design. 10 million dollars of CRF is dedicated to *EcSA Career Accelerator Incentives Fund (Thrive Incentives),* a program to provide financial support payments of $1,000 per month in incentives to individuals receiving career development assistance from the Thrive program to aid them in achieving suitable employment that provides a self-sufficient wage.

POLICY

Only participants enrolled in State Thrive are eligible for Thrive Incentives. All State Thrive participants receiving funding must be determined eligible based on the guidelines outlined and must be enrolled as participants in the State-funded Economic Security for All (EcSA) program in the Efforts to Outcomes (ETO) management system. All participant services received must be documented in ETO or its successor. All funds used must comply with the applicable state regulations, any additional guidance must be followed as it becomes available.

State Thrive participants may receive a $1,000/month incentive cash payment for meaningful progress made on their career plans each month, as determined by their case manager. Participants must continue to receive an incentive payment monthly while meeting eligibility requirements for as long as they are enrolled in the program and funding is available.

A. Participant Eligibility

To be eligible for Thrive Incentives, an individual must:

1. Be eligible for and fully enrolled in the State-funded Economic Security for All (EcSA) above or below 200% program,

2. Develop an Individual Employment Plan (IEP) with their case manager,
3. Meet at least monthly with their case manager to monitor their progress in training or job search,
4. If applicable, meet with external benefits manager to calculate impact of incentives,
5. Complete additional monthly Thrive activities outlined in their IEP.

B. Incentive Options

State Thrive participants are eligible to receive a $1,000 cash incentive payment based on continuing progress made on their career plans each month, as determined by their case manager.

PROCEDURES

Receiving Thrive Incentives does not negate the participant's ability to receive Program Support Services. Items such as rental assistance or other support made on behalf of the participant are supportive services, and therefore must be recorded and reported as such.

Thrive participants will be required to sign an acknowledgement form detailing the incentive program while developing their Individual IEP with their case manager. The form will be developed by the provider and will need to describe the potential impact to the participant's State and Federal assistance. Signed Form must be uploaded into ETO.

Documentation of the delivery and receipt of the incentive payment in the state MIS (ETO) is required.

1. Record eligibility with documentation in case notes.
2. Use "**Community Reinvestment Financial Support Payments**" touchpoint to record Thrive Incentive amount received and note progress made towards achievement of IEP.
    a. Note - this service will only be visible and selectable when the State EcSA Program is selected.
3. Select associated outcomes with supporting documents of attainment (copy of the credential/certificate/license, test scores/grades, case note, etc.) in "Community Reinvestment Financial Support Payments" touchpoint if applicable per participants IEP goals.

Any participant receiving a Thrive Incentive must accurately complete a W-9 form before incentive payments are made. Participants receiving more than $599.99 in incentive payments in one calendar year will be issued an Internal Revenue Service (IRS) Form 1099-MISC by January 31 for the prior calendar year in which incentives were provided for tax reporting purposes. Incentives are taxable miscellaneous income.

DEFINITIONS

Thrive Incentives - The provision of financial support payments of $1,000 per month in EcSA Career Accelerator Incentives to individuals receiving career development assistance from the EcSA program to aid them in achieving suitable employment that provides a self-sufficient wage.

REFERENCES/RESOURCES

- IRS - About Form 1099-MISC, Miscellaneous Information
- IRS - About Form W-9
- WorkSource Information Notice (WIN) 0129 Change 2 – State Guidance and Instructions for the State Economic Security for All (EcSA) Program

WEBSITE
http://workforcesw.org/providers#OperationsPolicies

INQUIRIES
Please contact Mando Antonino mantonino@workforcesw.org (360) 567-3185 for questions.