Southwest Georgia Workforce Development Board
Policy/Procedure Name: **Confidentiality and Security Policy & Procedure**
Policy/Procedure #: **WIOA-2020-073**
Effective Date: December 1, 2020
Revision: March 1, 2022

PURPOSE

The Southwest Georgia Workforce Development Board/City of Colquitt and WorkSource Southwest Georgia are committed to ensuring customer confidentiality and appropriate handling of sensitive information. The purpose of this policy is to specify the requirements for the use, storage, and security of sensitive and confidential information.

It is the policy of the Southwest Georgia Workforce Development Board (WDB)to protect the privacy of all applicants for program services, as well as the privacy of all customers and clients receiving program services. Personal information will be treated in the strictest confidence and will not be shared outside of the Southwest Georgia Workforce Development Board/City of Colquitt and WorkSource Southwest Georgia without written authorization, except for auditing purposes and other grantor-imposed information-sharing requirements.

The purpose of this policy is to describe how the WDB will protect all personally identifiable information (PII) on applicants and customers, and the consequences for not adhering to these safeguards.

BACKGROUND

Under the Workforce Innovation and Opportunity Act (WIOA), staff, contractors, and contractor's staff obtain personal and confidential information from individuals as part of eligibility determination and continuation of services. WIOA stipulates implementation of confidentiality policies and procedures. This policy is required to ensure that staff, contractors, and contractor's staff with access to applicant and/or participant information, maintain confidentiality of information to which they are privy.

ACTION REQUIRED

It is the WDB Staff and Contractor's responsibility to inform all staff of the policy and ensure adherence and accountability of its contents.

STATE POLICY

Reference Technical College System of Georgia, Office of Workforce Development (OWD) Policy and Procedure Section 4.5 Confidentiality and Security

ATTACHMENTS

- Attachment A: Staff/Contracted Staff Confidentiality Agreement
- Attachment B: Applicant/Participant Confidentiality Agreement
- Attachment C: Definition of Key Terms

LOCAL POLICY

CONFIDIENTIALITY

Respecting the privacy of our customers and protecting their confidential information is a critical part of providing services. WDB Board members, WDB Staff, contractors/service providers, consultants, volunteers and members of the Local Elected Officials Consortium (herein "Staff and Representatives") may be exposed to information which is confidential and/or privileged and proprietary in nature. As part of grant activities, Staff and Representatives may have access to large quantities of personally identifiable information (PII) relating to staff and individual program applicant and/or participants. This information could be found in personnel files, applicant or participant data sets, performancereports, program evaluations, grant and contract files, and other sources. (Ref. the definition of PIIin Attachment C-Definition of Key Terms)

The WDB expects all Staff and Representatives to respect the privacy of customers and to maintain their personal and financial information as confidential. Access to any PII must be restricted to only those Staff and Representatives who need it in their official capacity to perform duties pertaining to the scope of work in the grant or contract agreement. Information will be disclosed only on a "need to know" basis. No information may be released without appropriate authorization.

All Staff and Representatives are required to take aggressive measures to mitigate the risks associated with the collection, storage, and dissemination of sensitive data including PII. It is the policy of the Southwest Georgia Workforce Development Board (WDB) that such information must be kept confidential both during and after employment or volunteer service.

"Confidential" means that an individual is free to talk about WorkSource Southwest Georgia and about the programs, but an individual is not permitted to disclose customers' names or talk about them in ways that will make their identity known. No information may be released without appropriate authorization. WDB expects all its agents to respect the privacy of customers and to maintain their personal and financial information as confidential.

Access to any PII must be restricted to only those staff and representatives who need it in their official capacity to perform duties pertaining to the scope of work in the grant or contract agreement.

CUSTOMER AWARENESS

Individuals must be informed in writing via the Confidentiality Agreement in Attachment B that their information will be protected and that their personal and confidential information:

- May be shared among federal and state agencies, partner staff and contractors;
- Is used only for delivering services and that further disclosure of their confidential information is prohibited; and that
- PII will be used for grant and eligibility purposes only.

Staff and Representatives should engage in practical ways to reduce potential security breaches and protect sensitive information and PII by:

- Reducing the volume of collected and retained information to the minimum necessary;
- Limiting access to only those individuals who must have such access; and
- Using encryption, strong authentication procedures, and other security controls to make information unusable by unauthorized individuals.

PROTECTING INFORMATION

PII and confidentiality require special precautions to protect them from unauthorized use, access, disclosure, modification, and destruction. Confidentiality means that data, reports, and other outputs are safeguarded against unauthorized access. Staff and Representatives will exercise extreme care and caution when working with confidential information to ensure the privacy of the customer.

Customers may also request that normally-public information not be disclosed. Staff and Representatives should notify their direct supervisor so that the particular accommodation can be provided. The applicant or participant file must contain a description of the request and alsobe clearly marked as containing this special request.

Physical Data Protection Requirements

All sensitive or PII data obtained should be stored in an area that is physically safe from access by unauthorized persons at all times. Staff and Representatives should also ensure paper documents are secured in a manner so that unauthorized access (such as by individuals walking into the room) is unlikely. Staff and Representatives must not leave personal and confidential information left open and unattended.

When a staff or representative's desk is unattended, it is the staff or representative's responsibility to ensure that personal and confidential information, including PII, is in closed containers such as locked drawers or offices when not in use. This means that all documents containing personal and confidential information must not be left on desks, fax machines, printers, or photocopiers unattended. Desktops and computers will be kept clear of papers and/or files containing confidential information that are not being used. Desktops and computers will be kept clear of confidential information during non-business hours.

Any papers containing PII and/or confidential information are to remain in the offices of the WDB and/or contractor/provider except invoices may be transported directly to the City of Colquitt accounting offices, and, upon occasion, there may be other papers that must be transported to

other locations for a specific purpose and with the express permission of the Executive Director and/or City of Colquitt Manager.

Any participant files stored for performance or archiving purposes must be clearly marked as containing personal and confidential information. Staff and representatives should retain participant PII only for the period required for assessment or performance purposes.

When paper or disposable media copies of confidential information are no longer needed, they should be disposed of according to applicable State and federal record retention guidelines, and using appropriate methods (i.e., shredding on site, placing in a locked receptacle for shredding later, and otherwise ensuring they are not accessible to others) to maintain confidentiality.

Electronic Data Protection Requirements

To safeguard electronically stored data, each user will receive a designated and authorized log-on(s) and password(s) that restrict users to the applications or functions commensurate with their assigned responsibilities, supporting an appropriate segregation of duties. This is such that unauthorized persons cannot reasonably retrieve the information by means of a computer.

Computers should be used for business only and the computer monitor should be positioned such that unauthorized viewing is unlikely. In addition, the internet should also only be used for official business. The use of network activity may be monitored without staff's knowledge or consent. It is prohibited to download or install any software or program without consent from authorized personnel. Servers must contain anti-virus software that is updated automatically.

The WDB expects all Staff and Representatives to secure mobile equipment, such as laptop computers and other devices that may have PII stored on them in order to ensure confidentiality and security especially when approved to work from home and also when traveling for business. Devices should have screen savers with password protection and have automatic lock screen feature setup in order to safeguard when not in use. Any electronic files that are open on the desktop with PII should be closed and computers logged off when unattended to reduce inadvertent security risks. Accessing and storing data containing PII on *personally owned* equipment at off-site locations, such as the Staff and Representatives' home, and on non-managed IT services, such as Google or Yahoo, is prohibited.

Disaster and Emergency Conditions

During disaster or emergency orders including pandemics that require staff to work remotely, it is the responsibility of the staff to secure their electronic device(s) and data to ensure the confidentiality and security of the sensitive data including PII.

TRANSMISSION OF CONFIDENTIAL INFORMATION

Staff and Representatives should avoid communicating sensitive information or PII about an applicant or participant to partner agencies or other Staff and Representatives via email. All email messages must contain a confidentiality notice. Staff and Representatives must only communicate

sensitive information or PII through the WorkSource Portal system or other encrypted means and not through third party or personal email addresses.

PII and other sensitive data transmitted or stored on mobile data storage (such as thumb drives) must be encrypted. Staff and Representatives must not transmit unencrypted sensitive PII to any entity, including but not limited to the Technical College System of Georgia, Office of Workforce Development, WDB Staff, contractors/service providers, or Department of Labor.

Staff and Representatives should discourage applicants and/or participants from emailing personal and confidential information to their career counselors/case managers. If an applicant or participant sends a staff or representative PII via email, the staff or representative should immediately delete the emailand subsequently delete the email from the "Deleted Items" folder in their email.
Any information posted to social media sites is considered public record and is subject to public disclosure. No sensitive information or PII should be posted to social media sites.

Care shall also be taken to ensure that unauthorized individuals do not overhear any discussion of confidential information.

Confidential information or PII should not be discussed or disclosed in telephone conversations unless it is certain that the other party has authorized access to the information. Recording telephone conversations without the consent of the individuals begin recorded is prohibited.

SOCIAL SECURITY NUMBERS

Social security numbers are protected as high-risk information. When requesting an applicant or participant's social security number, Staff and Representatives should explain how the social security number willbe used and how the applicant or participant's privacy will be ensured.

Staff and Representatives must request an applicant or participant's social security number when offering thefollowing services:

- Staff-assisted service related to eligibility determination, job search activity, and employment;
- All training and educational services; and
- Self-services through WorkSource Southwest Georgia

However, an individual is not required to provide their social security number to receive WIOA services, and services cannot be denied to an individual due to their refusal to disclose their social security number (5 U.S.C. Section 552a Note).

Whenever possible, Staff and Representatives should use unique identifiers such as state ID numbers for applicant or participant tracking instead of social security numbers. While social security numbers may be needed for initial eligibility or performance purposes, a unique identifier should be linked toeach individual record and used thereafter. This includes such records as training or contract documents. If social security numbers are to be used for specific tracking purposes, they

must be stored or used in such a way that it is not attributable to the individual. For example, a training Document should not include the participant name and social security number, rather the participant name and a truncated social security number.

Social Security numbers may not be listed on anything mailed to a client or to another agency unless required by law, or the document is a form or application. Social Security numbers may not be left on a voice mail message.

MEDICAL AND DISABILITY RECORDS

Before requesting disability-related documentation, Local Workforce Development Area (LWDA) staff must have a necessary reason for requesting such documentation that is directly tied to eligibility determinations or provision of accommodation services. Examples of such reasons include, but are not limited to, the applicant requesting a reasonable accommodation that requires financial commitment from the LWDA or the applicant is a youth for which the disability is the main or only barrier to be considered for eligibility purposes.

In accordance with TEGL 23-19, there are only three types of documentation that should be used to validate disability status for eligibility purposes or proof of need for accommodation:

1. Self-Attestation;
2. School Section 504 records provided by the applicant or participant; or
3. Assessment test results.

The use of self-attestation as your first option to validate disability status without the need to gather additional disability-related documentation is recommended.

Any of the above documentation that is collected must be kept confidential, and any physical file should be stored in accordance with 29 CFR 32.15(d), as outlined below. For electronic files, the three disability-related documents listed above are the only three documents that should be uploaded in a participant's case file in the WorkSource Georgia Portal. These documents should only be collected and uploaded when such documentation is needed for an eligibility determination or proof of need for accommodation services. Once collected, all LWDAs must take steps to guarantee the security of such information as outlined in this policy.

In accordance with 29 CFR 32.15(d) (as incorporated by reference into the WIOA nondiscrimination regulations by 29 CFR 38.41(b) (3)), all records containing medical or disability related information, including information relating to an individual's disability status, must be:

A. Kept in separate files, apart from all other information about a particular individual;

B. Stored securely, with limited access; and

C. Available only to persons with a need to know, as provided in 29 CFR 32.15(d)(1) through (4).

Additionally, LWDA employees' medical information must be kept in a separate location from other employment or training records. These files must be kept in a medical file in a separate locked cabinet apart from the location of other personnel or training files.

When all WIOA or other WorkSource Southwest Georgia services are complete and the participant

file is ready to be archived, participant medical and disability-related information must be placed in a sealed envelope and marked "Medical and Disability Information."

DISASTER RECOVERY OF PAPER AND ELECTRONIC INFORMATION – FROM CITY IT DISASTER POLICY

In the event of a disaster, paper and electronic information will be able to be recovered per the detail below.

Paper/Physical
Paper/physical information is digitized and therefore stored with the offsite backups and available to be downloaded for recovery.

Electronic
Electronic information will be downloaded from offsite backups. This will occur from any location that has stable internet and a Southwest Georgia Workforce Development Board/City of Colquitt-controlled computer with enough free disk space to hold the data. Multiple downloads from multiple locations will be started if there are available resources to do so. Ideally the data will be downloaded locally and available for restoration by the time new hardware/equipment, if needed, arrives.

The Southwest Georgia WorkSource Development Board/City of Colquitt Staff will also coordinate vendor resources where vendor support teams for critical systems will be contacted, lined up to assist with restoring and configuring their systems, and waiting on standby.

In addition, the Southwest Georgia WorkSource Development Board/City of Colquitt Staff will assist with procurement of hardware/equipment, if necessary, such as desktop computers, monitors, printers, network equipment, and server hardware.

Once it arrives, the new server will be prepared with the installation of the operating system as well as the setup of any network services required to restore basic functionality. If the physical server will host virtual servers, the Hyper-V role will be installed and configured. The vendor support teams will be engaged as needed to configure these applications/systems.

The data will then be copied over to the new server and restored. The applications will be tested and proper operation will be verified. The desktop computers will also be setup along with the network (if necessary).

Lastly, the less critical data will be restored from the offsite backups (i.e. User's Documents, etc.) and the less critical hardware, if necessary, will be procured and deployed.

SECURITY BREACHES

Any Staff or Representative who becomes aware of any security breach resulting from the inadvertent or intentional leak of release of confidential information, including PII, shall immediately inform their direct supervisor. The WorkSource Southwest Georgia Executive Director and City of Colquitt Manager should also be immediately notified. PII security incidents include, but are not limited to, any event (intentional or unintentional) that causes the loss, damage, or destruction, or unauthorized access, use, modification, or disclosure of information assets. The system or device affected by a PII security incident shall be immediately removed from operation. It shall remain

removed from operation until correction and mitigation measures are applied.

Supervisors should assess the likely risk of harm caused by the breach and then assess the level of breach.

Four factors should be considered to assess the likely risk of harm:

- Nature of the Data Elements Breached
- Number of Individuals Affected
- Likelihood the Information is Accessible and Usable
- Likelihood the Breach May Lead to Harm

Notification and details of the security breach should be provided to WorkSource Southwest Georgia Executive Director and City of Colquitt Manager, within 24 hours, regardless of if the breach is believed to cause harm.

Within 48 hours, the WorkSource Southwest Georgia Executive Director and/or the City of Colquitt Manager will inform the Compliance Manager of TCSG – Office of Workforce Development of breaches believed to cause harm. Breaches subject to notification requirements include both electronic systems as well as paper documents.

Individuals assessing the likely risk of harm due to a security breach should exercise the objectivity principle, which requires individuals to show the highest professional objectivity level in collecting, assessing, and communicating information about the breach examined. Further, assessors are expected to perform a balanced assessment of every relevant situation and they must not be influenced by their own or other people's interest while forming judgments.

The notification should be provided in writing within 3 business days after investigation that should conclude no more than 48 hours after the initial report and should be concise.

The notice should include the following elements:

- A brief description of what happened, including the date(s) of the breach and of its discovery;
- To the extent possible, a description of the types of personal information involved in the breach (e.g., full name, Social Security number, date of birth, home address, account number, disability code, etc.);
- What the agency is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches.

A copy of the report should be distributed to the WorkSource Southwest Georgia Executive Director, City of Colquitt Manager and Southwest Georgia Workforce Development Board Chair.

To mitigate security impact any applicants or participants that may be impacted by the breach should be notified via US Mail as soon as the investigation is complete and the scope of breach is established.

STAFF COMPLIANCE

All WDB Staff and Contracted/Service Provider Staff with access to applicant and/or participant PII and/or confidential information must sign an acknowledgement that they have read the policy, understand the confidential nature of applicant and participant data and the potential sanctions for improper disclosure, and agree to abide by all other requirements and terms contained therein.

Unauthorized disclosure of confidential or privileged information is a serious violation of this policy. Any failure to comply with confidentiality requirements identified in this policy may result in termination or suspension of contract or employment, or the imposition of special conditions or restrictions to protect the privacy of applicants and participants or the integrity of PII data. Misuse, mishandling, unauthorized disclosure of confidential information and/or any other noncompliance with PII datasafeguards could lead to civil and criminal sanctions per federal and state laws.

Staff and Representatives are expected to return materials containing privileged or confidential information at the time of separation from employment or expiration of service.

ANNUAL RECERTIFICATION

All WDB Staff and Contracted/Service Provider Staff (that have access to applicant and/or participant PII and/or confidential information) will be required to review, sign and submit a Staff/Contracted Staff Confidentiality Agreement (Attachment A) at the beginning of each contracted program year. It will be the provider/contractor management staff's responsibility to collect and submit the completed agreements to WDB Staff.

MONITORING

The Southwest Georgia Workforce Development Board/City of Colquitt and WorkSource Southwest Georgia acknowledges that the U.S. Department of Labor and the State of Georgia have the authority to monitor and assess compliance with federal, state, and local confidentiality requirements. To ensure that policies are being followed and expectations are being met, WDB Staff or a designee will conduct onsite inspections periodically to ensure confidentiality compliance. It will be the responsibility of the contractor/service provider to make any corrections and to conduct an internal review if areas of concern are found.

DISCLAIMER

This policy is based on WDB's interpretation of the statute, along with the Workforce Innovation and Opportunity Act; Final Rule released by the U.S. Department of Labor, and federal and state policies relating to WIOA implementation. This policy will be reviewed and updated based on any additional federal or state guidance.

Southwest Georgia WORK SOURCE GEORGIA
Connecting Talent with Opportunity
A proud partner of the AmericanJobCenter network

REFERENCES

Law

- Workforce Innovation and Opportunity Act of 2014 (WIOA)
- Privacy Act of 1974, Section 7 – 5 U.S.C. Section 552a Note (Disclosure of Social Security Number)
- 29 CFR 38.41(b)(2)

Federal Guidance

- Training and Employment Guidance Letter (TEGL) 05-08 – Policy for collection and Use of Workforce System Participants' Social Security Numbers
- TEGL 39-11 – Guidance on the Handling and Protection of Personally Identifiable Information (PII)
- OMB Memorandum M-07-16 – Safeguarding Against and Responding to the Breach of Personally Identifiable Information

Southwest Georgia Workforce Development Board
Policy/Procedure Name: Confidentiality and Security Policy
Policy/Procedure #: WIOA-2020-073
Effective Date: December 1, 2020
Revision: March 1, 2022

STAFF/CONTRACTED STAFF CONFIDENTIALITY AGREEMENT

I,_____[print name] certify that I have read and understand the Southwest Georgia Workforce Development Board's (WDB) policy on **USE AND CONFIDENTIALITY OF APPLICANTS' AND PARTICIPANTS' PERSONALLY IDENTIFIABLE INFORMATION (PII)**. I understand that I may have access to customer and employer confidential records as part of my employment, contracting, or volunteer work with the WDB/Cityof Colquitt and/or Contractor/Service Provider. Confidential information provided by any applicant or participant or byany federal, state, or county entity is protected by law, regulation, and policy.

I understand that it is my responsibility as part of the workforce development system in Southwest Georgia to protect the confidentiality of all WorkSource Southwest Georgia applicants and participants. I understand that in the workforce system's collection, usage, storage and transmission of customer information, the tenets of confidentiality are to be strictly enforced.

I understand that I have the responsibility to know whether information is protected. If I have any questions regarding whether particular information is confidential, I understand it is my responsibility to check with my supervisor.

I understand that unauthorized access, use, modification, or disclosure of confidential information is a crime under state and federal laws. I understand that violation of this policy could result in:

- Disciplinary action
- Termination of employment
- Criminal action (including incarceration)
- Civil action

By signing below, I agree to follow and be bound by the terms and conditions regarding confidentiality of personal information contained therein. WDB Staff or their designee have answered any questions I may have had regarding this policy.

Signature: _____

Name:_____ Date: _____

APPLICANT/PARTICIPANT CONFIDENTIALITY AGREEMENT

Your privacy is one of our primary concerns. The Southwest Georgia Workforce Development Board (WDB)/City of Colquitt, WorkSource Southwest Georgia and Contractors/Service Providers make every effort to provide you with a safe and private environment. The information below explains what information we gather and how we use it. It applies to all Southwest Georgia Workforce Development Board (WDB)/City of Colquitt, WorkSource Southwest Georgia and Contractors/Service Providers uses of information and is intended to protect the confidentiality of all customer information.

Access to Data

For auditing and monitoring purposes, individuals' personal and confidential information may be shared among federal and state agencies, partner staff and contractors under the WorkSource Southwest Georgia umbrella. Access is for the purpose of determining compliance with, and ensuring enforcement of the provisions of the Workforce Innovation and Opportunity Act.

Use and Release of Data
Data will only be used for the purposes of verifying eligibility, delivering services, and verifying performance measures and data may be shared among federal and state agencies, partner staff and contractors/service providers. Any other use of individual data will require written consent from the customer or customer's parent/legal guardian. Upon request, data can be released to the subject of the information.

All sensitive individual data is stored in an area that is physically safe from access by unauthorized persons at all times and data transmitted electronically is encrypted.

Medical and disability records are additionally protected as confidential information. Any medical or disability records are kept separately in a secured physical and/or electronic location. Social security numbers are also protected as high-risk information. Whenever possible, staff and representatives will use unique identifiers to track individual status.

By signing below, I acknowledge that I have explained this agreement to the WorkSource Southwest Georgia affiliated customer.

Staff Printed Name: _____

Staff/Contractor Staff Signature:_____Date: _____

By signing below, I acknowledge that I have read and understand this agreement. Southwest Georgia Workforce Development Board/City of Colquitt Staff or Contractor/Service Provider Staff have explained this agreement and answered any questions I may have had.

Applicant/Participant Printed Name: _____

Applicant/Participant Signature:_____ Date _____

Parent/Legal Guardian Printed Name: _____

Parent/Legal Guardian Signature:_____ Date _____

Definition of Key Terms

Personally Identifiable Information (PII) as defined by OMB Memorandum M-07-16 is any information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal information that is linked or linkable to a specific individual.

There are two types of PII as defined by the U.S. Department of Labor in TEGL 39-11 that are based on the "risk of harm" that could result from the release of the PII:

- Protected PII – is any information that if disclosed could result in harm to the individual whose name or identify is linked to that information. Examples include, but are not limited to, place of birth, date of birth, mother's maiden name, driver's license number, biometric information, medical information (except brief references to absences from work), personal financial information, social security numbers (including only the last four digits), credit card or debit card account numbers, passport numbers, bank account numbers, potentially sensitive employment information (e.g. personnel ratings, disciplinary actions, and results or background investigations), criminal history, personal telephone numbers, marital status, spouse names, educational history, medical history, computer passwords and any information that may stigmatize or adversely affect an individual.
- Non-Sensitive PII – is information that if disclosed, by itself, could not reasonably be expected to result in personal harm as it is not linked or closely associated with any protected or unprotected PII. Examples include work and personal e-mail addresses, work addresses, work phone numbers, resumes that do not include a Social Security number or where the Social Security number has been redacted.

A combination of non-sensitive PII could potentially be categorized as protected PII. As example, a name and business e-mail address will not result in a high degree of harm to an individual. A name linked to a social security number and date of birth could result in identity theft.

A **Security Breach** as defined by TEGL 39-11 is used to include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.

Sensitive Information as defined by TEGL 39-11 is any unclassified information whose loss, misuse or unauthorized access to or modification of could adversely affect the interest of the conduct of Federal programs, or the privacy to which individuals are entitled under the Privacy Act.