pennsylvania
DEPARTMENT OF LABOR & INDUSTRY

DRAFT

PENNSYLVANIA WORKFORCE DEVELOPMENT SYSTEM OF RECORD

WORKFORCE SYSTEM POLICY
Workforce Development System Administration
Effective Date: Effective Upon Publication
Last Revised: June 4, 2020

Policy Owner: Pennsylvania Department of Labor & Industry Workforce Development Deputate (Bureaus of Workforce Development Administration, Partnership & Operations, and the Center for Workforce Information & Analysis)
Policy Contact: Pennsylvania Department of Labor & Industry Bureau of Workforce Development Administration Policy & Planning Coordination Services Unit, RA-LI-BWDA-Policy@pa.gov.

Purpose of the Policy

This policy establishes CWDS/PA CareerLink® as Pennsylvania's sole system of record for all Workforce Innovation and Opportunity Act, or WIOA, Title I, Wagner-Peyser Act (Title III), Apprenticeship and Training Office, or ATO, and Trade Act-related, or TAA, and as applicable, other federal or state workforce grants, program data and case-management activities.

Additionally, this policy establishes requirements for all grant subrecipients – to include local workforce development boards – for data security, personally identifiable information security, workforce-system data entry, user management, and tracking participants, employers and providers using Pennsylvania's system of record, the Commonwealth Workforce Development System, or CWDS, CWDS/PA CareerLink®.

Policy Statement

In the interests of accountability, accuracy and security of Pennsylvanians' personally identifiable information, the commonwealth establishes CWDS/PA CareerLink® as the sole system of record for participant data derived through WIOA, Wagner-Peyser Act, Apprenticeship and Training Office, TAA programs and as applicable, other federal and state-funded workforce development activity.

Scope

This policy applies to all employees within all bureaus, divisions, boards, commissions, councils, agencies and business partners supported by L&I-allocated workforce development funds. This includes any contracted employees employed by business partners supported by L&I-allocated workforce development funds (hereinafter referred to collectively as "CWDS/PA CareerLink® users").

Audience

This policy is for all employees within all bureaus, divisions, boards, commissions, councils, agencies and business partners supported by L&I-allocated workforce development funds. This includes any contracted employees employed by business partners supported by L&I-allocated workforce development funds (hereinafter referred to collectively as "CWDS/PA CareerLink® users").

Related Policies
Workforce System Common Identifier
Workforce Innovation and Opportunity Act Performance Reporting
Workforce System Sanctions

Definitions
Business partners are any entity identified by statute, regulation, or contract as being an agent of the commonwealth of Pennsylvania. A business partner connection is an interface (i.e. data connection) for connecting business partners to the Commonwealth of Pennsylvania, or CoPA, Network.

Commonwealth Workforce Development System, or CWDS, is the sole data-management and reporting system of record used for all data collection and reporting related to all WIOA Title I and Title III, Wagner-Peyser Act, Apprenticeship and Training Office, and Trade Act-related activity in Pennsylvania.

Cyber security incident is any occurrence involving the unauthorized or accidental modification, destruction, disclosure, loss, damage, misuse or access to information technology resources such as systems, files and databases.

Data are any recorded information, regardless of the form, the media on which it is recorded or the method of recording. Data are a value or set of values representing a specific concept or concepts. Data become "information" when analyzed and possibly combined with other data to extract meaning, and to provide context.

Data breach is the unauthorized access and acquisition of computerized data that may materially compromise the security or confidentiality of personal information maintained by the entity as part of a database of personal information regarding multiple individuals that causes, or the entity reasonably believes has caused or may cause, loss or injury to any resident of this commonwealth. Good faith acquisition of personal information by an employee or agent of the entity for the lawful purposes of the entity is not a breach of the security of the system, and is not subject to further unauthorized disclosure. (See U.S. Department of Labor Training and Employment Guidance Letter 39-11, PA Act 94, ITP SEC024 and ITP SEC025 for additional information.)

Documentation is all materials required to support and convey information about all aspects of program and service delivery, including materials, media and methods used to collect and store participant, program and provider data.

Grant recipient is local workforce development board members, staff, and fiscal agent staff.

Information is any communication or representation of knowledge such as facts, data or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative or audiovisual forms.

Intake/eligibility records are those documents or electronic forms used to collect and store participant information before entering data into CWDS/PA CareerLink® to determine WIOA Title I or other program eligibility. For example, the documents many PA CareerLink® Title I staff use to collect and store information during interviews with applicants that may later be handed off to office administrative staff to be entered into CWDS/PA CareerLink®.

Pennsylvania CareerLink®/PA CareerLink® is the registered, trademarked name of Pennsylvania's one-stop workforce development service-delivery system, including each one-stop center, comprehensive or otherwise, whether permanent, temporary, mobile, or fixed, and all aspects of the online system used by partners, contractors, individuals, training providers and employers.

Pennsylvania Department of Labor & Industry, or L&I, is legally designated by the governor to serve as the state workforce agency.

Personally identifiable information, or PII, is any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, education, financial and employment information. By way of further example, PII includes (but is not limited to):

- driver's license number or a state identification card number issued in lieu of a driver's license
- passport number
- identifying information that must be protected under any policy, law or other requirement applicable to an agency

Record is information, regardless of physical form or characteristics, that document a transaction or activity of an agency and that is created, received, or retained pursuant to law or regarding a transaction, business or activity of the agency.

Service organization control 2, or SOC 2, audit reports provide details about an organization's controls relevant to system security, availability, and processing integrity as they relate to PII and other data processed by these systems.

System of record/records system is an information technology resource used to generate either an electronic or physical record that is based on business rules and processes. For the purposes of this policy, "system of record" is CWDS/PA CareerLink®.

Procedures

Responsibilities

(a) CWDS/PA CareerLink® user responsibilities:
    (i) Comply with all L&I policies, OA ITPS, management directives, executive orders, laws, regulations and grant agreements.
    (ii) Report any violations of policies promptly to the local system administrator and Bureau of Workforce Partnership Operations Data Systems Management staff.
(b) CWDS/PA CareerLink® user management responsibilities:
    (i) Comply with all CWDS/PA CareerLink® and L&I policies, OA ITPS, management directives, executive orders and laws.
    (ii) Ensure CWDS/PA CareerLink® users comply with the policies.
    (iii) Adhere to this policy and any published procedures regarding CWDS/PA CareerLink® and workforce development programs supported by L&I-allocated funds.

Information Technology Policies

(a) Grant recipients must comply with the IT standards and policies issued by the Governor's Office of Administration, Office for Information Technology (located at

https://www.oa.pa.gov/Policies/Pages/itp.aspx), including the accessibility standards set out in IT Policy ACC001, Accessibility Policy. The grant recipient must ensure that all service delivery and program activity complies with the applicable standards.

Personally Identifiable Information

(a) Grant recipients must recognize that confidentiality of PII and other sensitive data is of paramount importance to L&I, and must be observed except where disclosure is allowed by prior written approval of L&I or court order or subpoena. By entering into a grant agreement with L&I, grant recipients are assuring L&I that all data exchanges conducted through or during performance of the grant will be conducted in a manner consistent with applicable federal and state law and United States Department of Labor Training and Employment Guidance Letter, or TEGL, No. 39-11 (issued June 28, 2012). All such activity conducted by L&I and grant recipients will be performed in a manner consistent with federal and state laws.

(b) Grant recipients must take the steps necessary to ensure the privacy of all PII obtained from participants and/or other individuals and to protect such information from unauthorized disclosure or release. Grant recipients must maintain such PII in accordance with the federal standards for information security described in TEGL No. 39-11 and any updates to such standards provided by L&I or the Governor's Office of Administration.

(c) Business partners and all staff with access to sensitive/confidential/proprietary/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.

User Management and Background Checks

(a) All grant recipients and business partners with access to the system of record must have a criminal background check conducted for all business partner users. Background checks are to be conducted via the Request for Criminal Record Check form and procedure found at https://www.psp.pa.gov/Pages/Request-a-Criminal-History-Record.aspx. The background check must be conducted prior to initial access and on an annual basis thereafter.

(b) Before the commonwealth will permit system of record access to grant recipients and business partners, the parties must provide written confirmation that the background checks have been conducted. If, at any time, it is discovered that an employee of the business partner or an employee of a subcontractor has a criminal record that includes a felony or misdemeanor involving terroristic behavior, violence, use of a lethal weapon, or breach of trust/fiduciary responsibility or which raises concerns about building, system or personal security or is otherwise job-related, the business partner must not assign that employee to any commonwealth facilities, must remove any system of record access privileges already given to the employee and must not permit that employee remote access unless the commonwealth consents to the access, in writing, prior to the access. The commonwealth may withhold its consent in its sole discretion. Failure of the business partner to comply with the terms of this section on more than one occasion or business partner's failure to cure any single failure to the satisfaction of the commonwealth may result in the business partner being deemed in violation of this policy.

(c) The commonwealth specifically reserves the right of the commonwealth to conduct or require background checks over and above that described herein.

(d) Access to any PII created by program operation must be restricted to only those employees of the grant recipient who need it in their official capacity to perform duties relation to the scope of work in the grant agreement.

(e) All CWDS/PA CareerLink® user credentials must be immediately disabled when employee access to CWDS/PA CareerLink® is no longer necessary to perform duties relating to the scope of work in the grant agreement.

(f) Access to any PII created by program operation must be restricted to only those employees of the grant recipient who need it in their official capacity to perform duties relating to the scope of work in the grant agreement.

(g) User credentials must be disabled by the appropriate local system administrator. If the local system administrator is not available, or is for any reason unable to disable the to-be-expired credentials, local staff must report the local system administrator's unavailability or inability to L&I Bureau of Workforce Partnership and Operations staff, at which time L&I staff must disable the to-be-expired credentials.

(h) All resources granted access to the system of record must be located within the United States. No contractors or other related resources will be given access to infrastructure, applications or IT environments.

Confidentiality, Privacy and Compliance

(a) Grant recipients must have policies and procedures in place under which grant recipients' staff and other personnel, before being granted access to PII, acknowledge their understanding of the confidential nature of the data and the safeguards with which they must comply in their handling of such data, as well as the fact that they may be liable to civil and criminal sanctions for improper disclosure.

(b) Grant recipients must not extract information from data obtained through program operations funded by L&I-allocated funds for any purpose not stated in the grant agreement.

(c) All non-commonwealth CWDS/PA CareerLink® users must adhere to the data-security standards established by L&I, OA/OIT and observed by commonwealth agencies.

(d) CWDS/PA CareerLink® user technology (hardware, software) used to enter, store, access, transmit and view participant data procured through workforce development activity funded by L&I allocations must comply with federal and state data-security statutes (NIST SP 800-53), requirements and policies.

(e) All PII data must be processed in a manner that will protect the confidentiality of the records/documents, and is designed to prevent unauthorized persons from retrieving such records by computer, remote terminal, physical reproduction, removal or any other means.

(f) PII data obtained by grant recipients must not be disclosed to anyone except the individual to whom it belongs (e.g. the recipient of services), except as permitted by L&I or required by a court order or subpoena.

Service Organization Control 2 Audit

(a) To ensure the protection of participant PII, L&I requires a third-party audit demonstrating SOC2 compliance to coincide with the establishment of a workforce development grant agreement.

(b) Local workforce development boards must maintain the SOC2 compliance report and provide it to L&I upon request. All business partners with a contract at the time of this policy's publication must demonstrate SOC2 compliance and provide a compliance report to the appropriate local workforce development board not later than one year from the date of this policy's publication.

Sole System of Record

(a) CWDS/PA CareerLink® is the sole system of record for the participant tracking of WIOA, Wagner-Peyser Act, Apprenticeship and Training Office, TAA programs and as applicable, other federal and state-funded workforce development activity. All participants, employers and providers served by these funding streams (for all levels of services, including career planning) must have their services and activities entered into CWDS/PA CareerLink® expeditiously and exclusively to ensure a common record and, when appropriate, assignment of a common exit date.

(b) PA CareerLink® merit and business partner staff must use CWDS/PA CareerLink® as the sole job-matching system when job seekers are looking for employment and employers are searching for candidates.

(c) CWDS/PA CareerLink® is the sole system of record for all financial reporting by local workforce development board staff regarding WIOA Title I, Wagner-Peyser Act, Apprenticeship and Training Office, TAA-funded programs and as applicable, other federal and state-funded workforce development activity.

(d) Requests for funds by local workforce development boards must be made using CWDS/PA CareerLink®.

Location, Status and Disposition of WIOA Title I, Title III, TAA Data and Documentation/Records

(a) All data must be stored within the United States.

(b) All grant recipients must maintain a record retention policy which contains a disposition plan.

(c) The business partner is responsible for maintaining the privacy, security and integrity of data, documentation and records in the business partner's possession.

(d) All data, documentation and records must be provided to the commonwealth, upon request, in a form acceptable to the commonwealth at no cost.

(e) Grant recipients must retain data received from programs funded by L&I-allocated funds only for the period required to use it for assessment and other purposes, or to satisfy applicable federal and state records-retention requirements, if any. Thereafter, CWDS/PA CareerLink® users agree that all data will be destroyed, including the degaussing of magnetic tape files, solid state devices and the deletion of electronic data.

(f) All temporary intake/eligibility records, of any format, used to triage participant intake before completing a final application for eligibility must be referenced to enter data into CWDS/PA CareerLink® within 10 days of creation. After use, the temporary intake/eligibility record must be destroyed. If the record is not used to determine eligibility within 10 days, the record must be destroyed.

(g) All records, of all formats, used to store participant or employer information in preparation for entry into CWDS/PA CareerLink® for legitimate purposes thereafter must be stored in a secure facility behind two or more levels of locked protection (e.g. inside a locked file cabinet located inside a locked room accessible only to staff/management with a work-related reason/clearance to access and view such records).

(h) Accessing, processing and storing of PII obtained as part of operating programs funded by WIOA, Wagner-Peyser Act, the Apprenticeship and Training Office, TAA programs and as applicable, other federal and state-funded workforce development activity on personally owned equipment, at off-site locations, (e.g. employees' homes and vehicles) and non-commonwealth managed IT services (e.g. Yahoo! mail or Gmail), is strictly prohibited unless approved in writing by L&I.

(i) All participant, employer and provider data that can be entered into CWDS must be entered into CWDS/PA CareerLink® within 15 calendar days of the actual date of occurrence or when the actual date becomes known (e.g. services and outcomes, including but not limited to: start date, hold date, entered employment, certifications, assessments, program exit dates, etc.).

(j) All data procured through programs funded by L&I-allocated funds are the property of the commonwealth of Pennsylvania, and may not be used for any purposes other than administration of WIOA Title I, Wagner-Peyser, Apprenticeship and Training Office, TAA-related programs and as applicable, other federal and state-funded workforce development activity.

Data Breach or Loss

(a) All business partners must comply with all applicable data protection, data security, data privacy and data breach notification laws, including but not limited to the *Breach of Personal Information Notification Act*, Act of December 22, 2005, P.L. 474, No. 94, as amended, 73 P.S. §§ 2301—2329.

(b) For data and confidential information in the possession, custody and control of the business partner or its employees, agents, and/or subcontractors:
   (i) The business partner must report any cyber security incident to the commonwealth within two (2) hours of when the business partner knows of or reasonably suspects such Incident, and the business partner must immediately take all reasonable steps to mitigate any potential harm or further access, use, release, loss, destruction or disclosure of such data or confidential information.
   (ii) The business partner must provide timely notice to all individuals that may require notice under any applicable law or regulation as a result of an Incident. The notice must be pre-approved by the commonwealth. At the commonwealth's request, business partner must, at its sole expense, provide credit monitoring services to all individuals that may be affected by any Incident requiring notice.
   (iii) The business partner is solely responsible for any costs, losses, fines, or damages incurred by the commonwealth due to Incidents.

(c) As to data and confidential information fully or partially in the possession, custody, or control of the business partner and the commonwealth, the business partner must diligently perform all of the duties required in this section in cooperation with the commonwealth, until the time at which a determination of responsibility for the incident, and for subsequent action regarding the Incident, is made final.

Technical Assistance

Technical assistance for CWDS/PA CareerLink® users is available through the L&I bureaus of Workforce Development Administration, Workforce Partnership and Operations, Apprenticeship and Training Office, and Pennsylvania OA/OIT.

Virus, Malicious, Mischievous or Destructive Programming

(a) The business partner is liable for any damages incurred by the commonwealth if the business partner or any of its employees, subcontractors or consultants introduces a virus or malicious, mischievous or destructive programming into the commonwealth's software or computer networks and has failed to comply with the commonwealth software security standards. The commonwealth must demonstrate that the business partner or any of its employees, subcontractors or consultants introduced the virus or malicious, mischievous or destructive programming. The business partner's liability must cease if the commonwealth has not fully complied with its own software security standards.

(b) The business partner is liable for any damages incurred by the commonwealth including, but not limited to, the expenditure of commonwealth funds to eliminate or remove a computer virus or malicious, mischievous or destructive programming that results from the business partner's failure to take proactive measures to keep virus or malicious, mischievous or destructive programming from originating from the business partner or any of its employees, subcontractors or consultants through appropriate firewalls and maintenance of anti-virus software and software security updates (such as operating systems security patches, etc.).

(c) In the event of destruction or modification of software, the business partner must eliminate the virus, malicious, mischievous or destructive programming, restore the commonwealth's software, and be liable to the commonwealth for any resulting damages.

(d) The business partner is responsible for reviewing commonwealth software security standards and complying with those standards.

(e) The commonwealth may, at any time, audit, by any means deemed appropriate by the commonwealth, any computing devices being used by representatives of the business partner to provide services to the commonwealth for the sole purpose of determining whether those devices have anti-virus software with current virus signature files and the current minimum operating system patches or workarounds have been installed. Devices found to be out of compliance will immediately be disconnected and will not be permitted to connect or reconnect to the commonwealth network until the proper installations have been made.

(f) The business partner may use the anti-virus software used by the commonwealth to protect business partner's computing devices used in the course of providing services to the commonwealth. It is understood that the business partner may not install the software on any

computing device not being used to provide services to the commonwealth, and that all copies of the software will be removed from all devices upon termination of the grant.

(g) The commonwealth will not be responsible for any damages to the business partner's computers, data, software, etc. caused as a result of the installation of the commonwealth's anti-virus software or monitoring software on the business partner's computers.

Oversight and Monitoring

(a) Grant recipients must permit L&I to make on-site inspection during regular business hours for conducting audits and/or other investigations to ensure that grant recipients are complying with the confidentiality requirements detailed in this policy. In accordance with this responsibility, grant recipients must make records applicable to programs funded by L&I-allocated funds available to authorized persons for inspection, review, and/or audit. This provision is immediately effective upon the date of this policy's publication.

(b) Local workforce development boards must make mention of their recognition of and adherence to this system of record policy in their own policies.

(c) All business partners with a contract at the time of this policy's publication must demonstrate full compliance and provide a compliance report to the appropriate local workforce development board not later than one year from the date of this policy's publication.

Resources

None.

Supporting Information

- Public Law (Pub. L.) 113-128, Workforce Innovation and Opportunity Act (WIOA)
- 20 Code of Federal Regulation (CFR), WIOA Final Rules and Regulations
- U.S. Department of Labor (U.S. DOL) Training and Employment Guidance Letter (TEGL) No. 10-16, Performance Accountability Guidance for Workforce Innovation and Opportunity (WIOA) Title I, Title II, Title III and Title IV Core Programs
- U.S. Department of Labor (U.S. DOL) Training and Employment Guidance Letter (TEGL) No. 39-11, Guidance on the Handling and Protection of Personally Identifiable Information (PII)
- U.S. DOL Training and Employment Notice (TEN) No. 09-13, Labor Exchange Reporting System (LERS) Tutorial and ET Handbook No. 406 Updates, Oct. 18, 2013.
- National Institute of Standards and Technology U.S. Department of Commerce *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
- Pennsylvania Department of Labor & Industry Workforce System Policy (WSP) No. 03-2015, Financial Management
- Pennsylvania Department of Labor & Industry PA CareerLink® System Procedure Manual
- L&I SEC-008 Security Incident Response Policy
- OA ITP INF000 Enterprise Data & Information Management Policy
- OA ITP SEC019 Policy & Procedures for Protecting Commonwealth Electronic Data
- OA ITP SEC024 IT Security Incident Reporting Policy
- OA ITP SEC025 Proper Use & Disclosure of Personally Identifiable Information (PII)
- OA ITP NET008 Telecommunications Services for Commonwealth Business Partners
- NIST SP 800-53 R4 Security & Privacy Controls for Federal Information Systems & Organizations

Policy History

This policy is published under the general authority of the Pennsylvania Department of Labor & Industry, or L&I, in consultation with the Governor's Office of Administration/Office of Information Technology, or OA/OIT.

Federal regulations require L&I to submit quarterly, accurate participant reports and validate individual participant data, as well as financial reports to the U.S. Department of Labor. Under WIOA, and as part of these reporting requirements, the U.S. Department of Labor encourages coordination and co-enrollment among WIOA, Wagner-Peyser Act, Apprenticeship and Training Office, and TAA programs to ensure a common record is maintained for each participant served with these funding streams.

Pennsylvania's workforce development data-management system of record, CWDS/PA CareerLink®, in compliance with federal and state data-security statutes, regulations and policy, is the sole system of record for all Title I, Title III, registered apprenticeships, TAA and, as applicable, other federal discretionary grants, state-funded workforce development activity in Pennsylvania. To ensure compliance with federal and state statutes, regulations and policies, all workforce development activity – including, but not limited to – participant and employer registrations and enrollments, job postings, individual employment plans/service strategies, Eligible Training Provider List provider service applications, job matching, career planning, case progress notes, documenting program referrals, activities and outcomes pertaining to workforce programs funded through the authorization of WIOA, Wagner-Peyser Act, Apprenticeship Training Office, TAA-related grants and as applicable, other federal and state-funded workforce development activity and any and all data derived through participation, or in anticipation of participation in workforce development activity funded by L&I allocations must be entered into CWDS/PA CareerLink® and only CWDS/PA CareerLink®. Attachments to this document are citations of the relevant federal and state statutes, regulations and policies.

Summary of Changes

Revision Date	Author	Description
Jan. 29, 2019	L&I BWDA	Base Document/Initial Draft
Sept. 17, 2019	L&I BWDA	Format and Content Revision
Nov. 16, 2019	L&I BWDA	Data Security Info. Incorporated
Nov. 16, 2019	L&I BWDA	Format Revision
Dec. 17, 2019	L&I BWDA	WFD Deputate Supervisor Comments Incorporated
Jan. 28,2020	L&I BWDA	WFD Deputate Chief Comments Considered and Incorporated
Feb. 14, 2020	L&I BWDA	Format Revision; CWIA Bureau Director Comments Considered and Incorporated
April 3, 2020	L&I BWDA	Format Revision
April 20, 2020	L&I BWDA	Added (h) under User Management & Background Checks; added NIST *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* to resources.
June 4, 2020	L&I BWDA	Added contact information.

Public Comment

This policy has not yet been published for public comment.