POLICIES AND PROCEDURES

POLICY TYPE:	Protection of Confidential information and Data Policy
EFFECTIVE:	July 1, 2017
REVISED:	

REFERENCES:
TEGL 39·11 Handling and Protection of Personally Identifiable Information (PII)
2 CFR 200.79 Personally Identifiable Information
CCWO OED Joint Policy; Confidentiality and Access to Information and Data
Oregon Revised Statutes 192.001, Protection and Storage of Public Records
Oregon Revised Statutes §162.425, Misuse of Confidential Information –
Oregon Revised Statutes 657.665 Confidentiality of Information
Oregon Revised Statutes §676.177, Interagency shared Information System –
Oregon Revised Statues. §660.339, Participant records
Oregon Administrative Rule 471-010-0105. Customer Information and Disclosure
Oregon Administrative Rule 589-020.0320. Authority to Request Social Security Numbers;
Oregon Administrative Rule 589-020-0330 Confidentiality

PURPOSE
To establish guidelines and instruction for Service Providers, One-Stop Centers. and WorkSource Oregon Partners related to the protection of confidential job seeker, employer and wage information, in carrying out official duties for the workforce system.

BACKGROUND
Protected Personally Identifiable Information (PPI) OMB defines PPI as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal identifying information that is linked or linkable to a specific individual. Any information that if disclosed could result in harm to the individual whose name or identity is linked to that information. Examples of protected PPI include but are not limited to social security numbers (SSN), credit cards numbers, bank account numbers, ages, birthdates, medical history, financial history and computer passwords.

As an important and inherent part of the services provided to customers, Service Providers and WorkSource Lane staff must necessarily collect a wide variety of Protected Personally Identifiable Information PPI from customers. While the information collected as a matter of routine is often critical to effectively serving our customers and providing them with the best possible services, collection of protected PPI also brings with it a statutory responsibility to safeguard customers' protected PPI form unauthorized use or disclosure.

The purpose of this policy is to identify sources of confidential information and to establish procedures for safe handling of this information so it is not accessed by unauthorized users. Maintaining

confidential records is important for obvious reasons to the individual, including the prevention of identity theft.
While the sharing of information even the PPI information of particular customers under appropriate circumstances is critical to the seamless and effective delivery of services envisioned by the enactment of the Workforce Innovation and Opportunity ACT and vital to successfully carrying out the mission of the system's various partnering organizations. Protecting the confidentiality of customer information accessed by staff in carrying out official functions of the workforce system, is imperative to its overall integrity.

Policies and procedures regarding confidentiality and data access therefor must ensure that all necessary and legally permissible data are available to all staff and partner staff who legally authorized to make use of the data in the discharge of their official duties.

Service Providers and Workforce staff needs to be aware that information and data included in Oregon workforce and employment management information systems databases as well as other information data sources available through other partners, such as the Department of Human Services (DHS), the Oregon Employment Department UI, etc. is subject to the requirements of these confidentiality statues. Particular care must be taken to assure that the information and data accessible through the MIS system as well as other data and information sources accessible by Services Providers and staff is protected and sued appropriately.

Although an employee may be authorized to access confidential data, the employee may access the data only in connection with the performance of his/her official duties.

POLICY
As used in this policy the term confidential refers to entire record systems, specific records or individually identifiable data that are not subject to public disclosure under Oregon Revised Statutes 192, Records, Public Records and Meetings. When applicable, confidentiality covers all documents, papers, hard copy participant files, computer files, letters and all other notations of records or data that are designated by law as confidential.
Documents that contain protected PPI (participant or family members) social security numbers, driver's license, birth certificates, I-9 documents, TANF/FSUP, etc., must be stored in a confidential, locked file cabinet which is only accessible by appropriate staff, kept separate from the working files. The working file should never contain any PPI documents.
Computers that have access to customer data should be locked when not in use and anytime a staff person is away from their workstation.
Service Providers and WorkSource staff will maintain and protect the confidentiality of PPI information in accordance with this policy, Federal and State of Oregon statutory requirements.
Given the integration and merging of services within the WorkSource Centers, confidential information that is received by one WorkSource Oregon partner from another partner agency retains its confidentiality unless otherwise provided by law. The requirement of the program that provides the information shall apply.
In Oregon, the initial participant's electronic information data is stored in WOMIS on servers maintained by OED and administered under the rules of the Oregon Department of Administrative Services (DAS) WIOA participant's electronic information is kept secure on the I-Trac data servers and administered by Worksystems Inc. Currently Service Providers and OED staff can only access the

data on the servers after successful completion of DAS Information Security Testing and I-Trac User and Confidentiality Training. No one should be given access to either WOMIS or I-Trac that have not completed the appropriate training and have signed the appropriate confidentially disclosure. All staff with access to either system must follow the procedures set out by the administering agency, ensuring that all staff understanding of data confidentiality.
At no time should a WorkSource Lane staff make a working file that contains any PPI information.

ACTION:

All Lane WorkSource Service Providers shall follow this policy.

- Service Providers must assure that all confidential information is scanned to Lane Workforce Partnerships secure data system (Ebridge) and no copies of confidential information is kept outside of the electronic file.
- If there are working documents that need to be kept for carrying out service delivery whether participant or business, the documents must be kept in a separate locked file cabinet with limited access, only be retrieved for official use, and returned to the locked file. At no time should this data be kept on a staff's desk, or in an unlocked file cabinet.
- All documents must be destroyed on the same maintenance and destruction schedule as set out by law.

ISSUED:

Date: **LWP Director of Workforce Investments**