DATE:       July 19, 2016

TO:         LA’s Workforce Development System

FROM:       Jaime H. Racheco-Orozco, Director
            Workforce Development System

SUBJECT:    WDS DIRECTIVE NO: 17-02
            JOBSLA/CALJOBS® DATA ENTRY STANDARDS

EFFECTIVE DATE
This directive is effective upon date of issuance.

PURPOSE
The purpose of this directive is to provide guidance and procedures regarding new
JobsLA/CalJOBS® data entry standards.

BACKGROUND
As part of its grant activities, the City of Los Angeles Workforce Development System
(WDS) may have in its possession large quantities of PII relating to their organization
and staff, partner organizations and their staff, and individual program participants. This
information is generally input into the JobsLA/CalJOBS® system. Development and
review of confidentiality and security laws and procedures should include active
participation from relevant stakeholders.

POLICY
All WIOA-funded contractors are required to report individual participant data via
CalJOBS® through the JobsLA portal. The City of Los Angeles requires all data entered
into the JobsLA/CalJOBS® to be accurate, timely and complete. All staff certified to
receive access to the JobsLA/CalJOBS® system must agree to the following:

- Meet the data entry submission requirement of 30 days
- Ensure the privacy of all Personally Identifiable Information (PII)
- Guard against intentional misreporting or potential fraudulent data entry
- Comply with certain provisions of California Penal Code 502(c) – Comprehensive
  Computer Data Access and Fraud Act

This WIOA Title I financially assisted program or activity is an equal opportunity employer/program.
Auxiliary aids and services are available upon request to individuals with disabilities.
**PROCEDURES**
The procedures below identify data entry elements and required actions users must take to ensure data integrity as well as data controls.

After reading, acknowledging and understanding the content of the City of Los Angeles Data Entry Standards Form, all staff certified to receive access to the JobsLA/CalJOBS™ system must sign and submit it to the LA City MIS training coordinator.

**Data Entry Elements and Required Action**

- **Computer Crimes:** User must immediately report any suspected computer misuse or crimes to their manager and/or the City.
- **Security Access Controls:** User will not bypass any security measure or system which has been implemented to control or restrict access to computers, networks, systems or data. User will not share log-in ID, computer access codes, account codes, or passwords.
- **Approved Business Purposes:** The JobsLA/CalJOBS™ system is to be used for approved business purposes only.
- **Confidentiality:** User will not access or disclose any LA City program code, data, information or documentation to any individual or organization unless specifically authorized to do so by the recognized information owner.
- **Computer Virus and Malicious Code:** User will not intentionally introduce any computer virus, works or malicious code into any WIOA computer, network, system or data. User will not disable or delete computer virus detection and eradication software on WIOA computers, servers and other computing devices.
- **Offensive Materials:** User will not access or send any offensive materials, e.g., sexually explicit, racial, harmful or insensitive text or images, over WIOA owned, leased or managed local or wide area networks, including the public Internet and other electronic mail systems, unless it is in the performance of the user's assigned job duties, e.g., law enforcement. User will report any offensive materials observed or sent to the supervisor.
- **Public Internet:** User understands that the Public Internet is uncensored and contains many sites that may be considered offensive in both text and images. The user will utilize LA City Internet services for approved City business purposes only, e.g., as a research tool or for electronic communication. User understands that the City’s Internet services may be filtered but can still expose the user to offensive materials. User agrees to hold the City harmless to the inadvertent exposure to such offensive materials. User understands that their Internet activities may be logged, are public record, and are subject to audit and review by authorized individuals.
- **Electronic Mail and Other Electronic Data:** User understands that City electronic mail (e-mail) and data, in either electronic or other forms, are a public record and subject to audit and review by authorized individuals. User will comply with City e-mail use policy and proper business etiquette when communicating over e-mail systems.
- **Copyrighted Materials:** User will not copy any licensed software or documentation except as permitted by the license agreement.
• Disciplinary Action for Non-Compliance: User understands that non-compliance with any portion of this agreement may result in disciplinary action including suspension, discharge, denial of service, cancellation of contracts, or both civil and criminal penalties.

REQUIRED ACTION
• All active users identified in the JobsLA User Account spreadsheet will need to sign and date the City of Los Angeles Data Entry Standards form, indicating that they have read, understand, and will comply with the City of Los Angeles Data Entry Standards Policy. The signed forms must be delivered to:

   Economic and Workforce Development Department
   Emoli Mendez, MIS Administrator
   1200 W. 7th Street, 6th Floor
   Los Angeles, CA 90017

• Beginning July 1, 2016, all staff certified to access to the JobsLA/CalJOBS® system must sign and submit the City of Los Angeles Data Entry Standards Form (attached) and submit it to the LA City MIS training coordinator after they complete the JobsLA/CalJOBS® data entry training course.

EWDD CONTACT
Questions regarding this directive should be directed to Emoli Mendez at emoli.mendez@lacity or at (213) 744-7167, TTY (213) 744-9395.

JHP:GR:EM
Attachments: City of Los Angeles Data Entry Standard Form
California Penal Code 502(c)
CITY OF LOS ANGELES DATA ENTRY STANDARDS

The City of Los Angeles has established data entry standards to:

- More accurately track WIOA participant activity
- Protect participant Personally Identifiable Information (PII)
- Guard against potential fraudulent data entry/reporting

POLICY

All data entered into the JobsLA system must be accurate, timely and complete. All staff certified to receive access to the JobsLA system must agree to the following:

- Meet the data entry submission requirement of 30 days.
- Ensure the privacy of all PII obtained from participants and to protect such information from unauthorized disclosure.
- Input data accurately to avoid potential fraudulent data entry/reporting.

I have read and understand that I must comply with the provisions of CA PC 502c California Penal Code 502(C) – Comprehensive Computer Data Access And Fraud Act

I understand that the data entry of fraudulent information into the JobsLA system may result in criminal action.

Agency Name

Staff Name (Print)

Staff Signature

Date
CALIFORNIA PENAL CODE 502(c) – COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT

Below is a section of the penal code as it pertains specifically to this policy. California Penal Code 502(c) is incorporated in its entirety into this policy by reference and all provisions of Penal Code 502(c) apply.

1. Knowingly accesses and without permission alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data.

2. Knowingly accesses and without permission takes, copies or makes use of any data from a computer, computer system, or computer network, or takes or copies supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network.

3. Knowingly and without permission uses or causes to be used computer services.

4. Knowingly accesses and without permission adds, alters, damages, deletes, or destroys any data, computer software, or computer programs which reside or exist internal or external to a computer network.

5. Knowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network.

6. Knowingly and without permission provides or assists in providing a means of accessing a computer, computer system, or computer network is in violation of this section.

7. Knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network.

8. Knowingly introduces any computer contaminant into any computer, computer system, or computer network.