Fresno Regional Workforce Development Board

A proud member of America's Job Center of California℠ Network

2125 Kern Street, Suite 208 • Fresno, California 93721 • 559.490.7100 • Fax 559.490.7199 • www.frwdb.net

Blake Konczal, Executive Director

OPERATIONAL DIRECTIVE

FRWDB OD # 08-23 Rev A **Date Released: February 7, 2024**

To: All Fresno Regional Workforce Development Board Providers of Services

From: Blake Konczal, Executive Director

Effective Date: February 7, 2024

Subject: Information Systems Security

Applicable Program: All, FRWDB Staff

Revision History: Initial Release – 6/30/23.

Revision A adds required language from Training and Employment Guidance Letter (TEGL) 39-11, and revises the FRWDB contact staff.

OVERVIEW:

This Directive is for the purpose of providing requirements and guidance to all Fresno Regional Workforce Development Board (FRWDB) staff and contracted sub-recipients, regarding FRWDB data and Information Systems resources.

This Directive:

- Incorporates and obsoletes Policy Bulletin (PB) # 01-18, Handling and Protection of Personally Identifiable Information Policy
- References Office of Management and Budget (OMB) Guidance 2 CFR Sec. 200.79
- References Operational Directive (OD) 07-23, FRWDB Confidential Information
- References the America's Job Centers of California (AJCC) Operations Manual
- References OD 06-23, Designation of Information Security Staff
- References OD 10-12, Closed Case File Retention and Storage
- References PB 05-06, Information Technology Standards Policy
- References TEGL 39-11

SCOPE:

This Directive falls within the scope of PB 05-06 and addresses secure access and use of FRWDB technology resources, and use and retention of electronic FRWDB data.

CONFIDENTIALITY:

All technology systems and users within the purview of FRWDB will assure the highest degree of confidentiality with respect to information input and/or stored on hardware or in databases utilized by the system. There will be no exchange or divulgence of participant information without first obtaining written approval from the participant. Likewise, the programs utilized by the system will not be compromised by

disclosure to unauthorized parties. In all cases, information regarding or residing in the system will only be available to others on a pre-authorized, need-to-know basis.

FRWDB, will ensure that no information is extracted from data supplied by ETA (state or federal grantor) for any purpose not stated in the grant agreement.

DEFINITIONS:

The definitions provided in PB 05-06 are applicable here with the following additions:

- **Data** includes facts and statistics collected together for reference or analysis. Within the purview of FRWDB business and services, data includes but is not limited to:
    - Employee Data: Information about employees who work for the Fresno Area Workforce Investment Corporation (FAWIC) and its contractors.
    - Personal Data: Information about an employee that is personal in nature and not necessarily related to employment.
    - Client Data: Information about AJCC customers, WIOA enrolled participants, and special grant enrollees or participants.

- **Documents** include items of electronic or hard copy format that may contain data as defined above. Includes e-mail, all types of formatted electronic files that are created or maintained with software, printed or handwritten hard copies.

- **Breach** is when it is known or suspected, that Protected Personally Identifiable Information (PII) has been released as a result of any of the following incidents:
    - Theft of hardcopy documents that contain Protected PII.
    - Missing computer known to contain Protected PII.
    - Missing storage device known to contain Protected PII.
    - Evidence of non-authorized access to network resources that contain Protected PII. This includes and is not limited to e-mail, databases, server-based folders and documents, cloud drives, folders, and documents.

- **Encryption** is the process of converting information or data into a code to protect the document from being read by unauthorized persons or software.

- **Personally, Identifiable Information (PII)** means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information. There are two (2) levels of PII:
    - Protected PII: Information that if disclosed, could result in harm to the individual whose name or identity is linked to that information. Examples of Protected PII are: Social Security Numbers (SSNs), credit card numbers, bank account numbers, home telephone numbers, ages, birthdates, marital status, spouse names, educational history, biometric identifiers (fingerprints, voiceprints, iris scans, etc.), medical history, financial information and computer passwords.

    - Non-sensitive PII: Information that, if disclosed by itself, could not reasonably be expected to result in personal harm. It is information that is not linked or closely associated with any protected or non-protected PII. However, depending on the circumstances, a combination of these items could potentially be categorized as protected PII. Examples of Non-Sensitive PII are: first and last names, physical addresses (in most cases), e-mail addresses, business addresses, business telephone numbers, general education credentials, gender, or race.

HANDLING PROTECTED PII:
Social Security Numbers are not to be used as identifiers for individuals and staff. Other data items such as employee number, user ID, state ID, WIOA app number, etc., shall be used.

- **Verbal PII**
  - Conversations that include Protected PII or Non-Sensitive PII should be conducted in a discrete manner so as not to disseminate any PII unintentionally to unauthorized persons.
  - Conversations include but are not limited to, discussions in open areas (i.e. breakrooms, hallways), telephone calls using a speaker phone and video conferencing.

- **Hardcopy PII**
  - Must be placed in an area that is physically safe from access by unauthorized persons at all times.
  - Protected PII shall not be left unattended.
    - Must be stored in locked cabinets or areas when not in use.
  - When utilizing a photocopier to scan or copy documents containing Protected PII, the equipment and documents are never to be left unattended.
    - Secure printing (ability to "print to hold" and/or "password protected") shall be used whenever possible.
    - Where secure printing is not available, documents with Protected PII shall not be printed in an unsecured area.
  - Disposing of Protected PII documents shall be done by depositing into identified locked disposal receptacles, i.e. shredding bins.
  - Archived Documents - All Providers of Services are required to ensure all archived files are maintained in locked storage and disposed of in accordance with OD 10-12, Closed Case File Retention and Storage.

- **Electronic Protected PII**
  - Storage of electronically protected PII
    - Upload client documents to CalJOBS as per current Operational Directives.
    - Temporary or permanent storage of electronically protected PII must only be done in a secure folder in which the file itself is encrypted.
  - Protected PII is not to be transmitted via email.
  - Scanning hardcopy documents:
    - May be scanned directly into a temporary network folder or a flash drive directly connected to the scanner.
    - The document must be deleted immediately after moving to secure storage.
  - When electronic Protected PII must be transmitted between authorized personnel, a secure method must be used. Examples of secure file-sharing methods are:
    - Secure File Transfer Protocol (SFTP).
    - FRWDB's current file-sharing application.
    - Utilization of the organization's secured shared network folders.
    - Secure, encrypted, flash memory (USB stick).
  - Computers are to be locked when unattended.
    - Either the user logged off or the computer access is locked.
  - All computer servers containing databases with Protected PII and network firewalls (software/hardware) must be in a physically secured location only accessible by authorized Information & General Services personnel.
  - All Protected PII data collection interfaces and reporting tools, accessible via the Internet must utilize secure, encrypted protocols (i.e. https).
  - Accessing, processing, and storing of Protected PII data on personally owned equipment, at off-site locations e.g., employee's home, personal email, Cloud services (such as iCloud) is strictly prohibited.

IN CASE OF BREACH:

Definition: A breach is when it is known or suspected that Protected PII has been released as a result of any of the following incidents:

- Theft of hardcopy documents that contain Protected PII,
- Missing computer is known to contain Protected PII,
- Missing storage device known to contain Protected PII, or
- Evidence of non-authorized access of database(s) or electronic files that contain Protected PII.

In the event of a breach, staff must contact their immediate manager or supervisor (in the manager's absence). The manager or supervisor must determine whose and what data was released and how it was released.

Information & General Services management is contacted and provided information regarding the released data. Information & General Services management will perform a damage assessment and develop an Action Plan:

- To contain further loss.
- To recover Protected PII, if possible.
- For notification:
  - Affected staff, partners, and/or participants,
  - State (if required),
  - Chief Local Elected Officials (if required).

NETWORK AND DEVICE SECURITY:

The FRWDB utilizes multiple platforms for the purpose of monitoring network resources for indications of malicious behavior. Software is installed at multiple levels of the network to the level of the domain user client device. To ensure our security is not circumvented, either purposefully or inadvertently, the following is required:

- Any network device connecting to our domain must have our security software installed.
- All network equipment and servers must be physically secured and only accessible by authorized personnel.
- Documented account passwords must be stored securely in a locked drawer and/or encrypted file.
- Security awareness training for domain users utilizing our current training tool.
- Service Provider must have on file signed staff Confidential Information Acknowledgement Forms.
- FAWIC staff acknowledgment is imbedded with the FAWIC Personal Manual.

BRING YOUR OWN DEVICE (BYOD):

It is understood that customers, guests, and staff may access our network to use the internet utilizing a mobile device. Users may access FRWDB secure wireless access points but shall not log in to the domain. Guest access to the internet outside domain access will be made available for this purpose.

ELECTRONIC MAIL (E-MAIL):

E-mail is used by all staff to communicate. It is important to understand that e-mail presents a threat to the network and PII security. E-mail is one of the few methods bad actors can use to directly access our network to potentially initiate malicious behavior. This behavior could result in the loss of protected PII and secure use of our network resources. Additionally, bad actors can utilize a compromised network and e-mail to extend their reach to organizational stakeholders and partners. It is extremely important to exercise awareness and caution when using organizational or personal e-mail.

Regarding e-mail use:

- Participate in the mandated domain user security awareness training as communicated in IB 06-17, E-mail Security Awareness Training.
- Be knowledgeable about identifying phishing e-mails and report them when possible and delete them without opening attachments or clicking on links.
- Clean out your e-mail.
- Don't retain e-mail for extended periods of time.
- When the use of a message is complete, delete the e-mail message.
    - If a message is of future importance, it is best to save the message to a designated folder in your documents folders. This prevents unnecessary use of space in the e-mail server and places the message in a more secure location.
    - Archiving e-mail is a method to automatically move old e-mails to a special mailbox to free up space on the server. Contact the help desk to obtain assistance in setting up an e-mail archive.
- At no time shall protected PII be transmitted via e-mail or retained within your e-mail account.

At no time shall offensive language or images be transmitted via e-mail. Organizational e-mail should only be used for professional work purposes.

OFFICE BEHAVIOR:

Security-conscious office behavior is outlined in the AJCC Operations Manual. The IT Cybersecurity sections communicate behavior that secures PII and workstations. All staff shall adhere to the Manual.

DOCUMENT RETENTION:

This section references all electronic documents (e-mail or files) including those that do not contain protected PII. Thoughtful document retention keeps unnecessary files from being retained for no valid reason. The solution for a mailbox that has reached the appropriate space is not to create more space. Removal or archiving e-mail messages or electronic documents is a good practice and should be followed by all staff and management on the FRWDB network and e-mail server.

Permanently delete e-mail (in mailbox or archive) or documents that are older than five (5) program years old, if unsure of specific document retention requirements.

ADHOC AUDITS:

The FRWDB will provide access to ETA to make onsite inspections during regular business hours for the purpose of conducting audits and/or conducting other investigations to assure that the FRWDB is complying with the confidentiality requirements described above. In accordance with this responsibility, records that are applicable to this Agreement will be available to authorized persons for the purpose of inspection, review, and/or audit.

Please address any questions to the FRWDB Deputy Director of Information and General Services.