OPERATIONS MANUAL CHAPTER 10: PRIVACY AND SECURITY

Revised February 2019

TABLE OF CONTENTS

I. INTRODUCTION

The San Diego Workforce Partnership (SDWP) Operations Manual provides detailed requirements, instructions, and policy guidelines for the management of funded programs. The purpose of this chapter is to (1) identify the protocols that all funded programs must have in place to follow SDWP policy for protecting the confidentiality of Personally Identifiable Information (PII) and (2) communicate actions that each program must undertake to actively protect this PII.
For purposes of this policy and SDWP's use and disclosure procedures, the workforce includes individuals who would be considered part of the workforce such as employees, contractors, volunteers, interns, board members and other persons whose work performance is under the direct control of SDWP, whether or not they are paid by SDWP. The term "employee" or "staff member" includes all of these types of workers. No third-party rights (including but not limited to rights of participants, beneficiaries, covered dependents, or business associates) are intended to be created by this Plan.

A. NETWORK AND SUBRECIPIENT EQUIPMENT REQUIREMENTS

1. AJCC Network

The AJCC network and computers are procured and supported by SDWP and as such are compliant with the requirements in this policy. AJCC operator(s) may have cell phones, tablets, or other mobile device which are procured and supported by their company. If these devices are used to access program data, then the devices are also subject to the technical requirements laid out in this policy. Using personal devices to access program data is not allowed.

The AJCC Network and users are required to adhere to the **ATTACHMENT - AJCC WI-FI USAGE POLICY, ATTACHMENT- TECHNICAL SUPPORT BETWEEN SDWP AND AJCC OPERATOR, AND COMPLETE ATTACHMENT - AJCC E-MEDIA POLICY ACKNOWLEDGMENT FORM.** This includes a description of the technical services provided by the SDWP to the AJCC Operator. Also included are the AJCC Operator's responsibilities to the SDWP.

2. Subrecipients

Subrecipients computers, cell phones, tablets, and other related equipment are acquired with SDWP funding but not directly procured or supported by SDWP IT staff. Wherever such equipment is used by the sub-recipient to operate programs and or to access program data, then the devices are also subject to the requirements laid out in this policy.

B. PERSONALLY, IDENTIFIABLE INFORMATION (PII)

Personally Identifiable Information (PII) is any information that identifies or describes an individual. This includes any information that can (a) distinguish an individual's identity such as name, place and date of birth, passport or social security number, biometric records or (b) be linked to an individual such as educational, employment, financial, medical information.

Based upon State (Information Practices Act of 1977 (IPA)) and Federal standards (Fair Information Practices), SDWP stipulates that all funded programs are expected to protect personal information they maintain that identifies or describes an individual. The following examples of information can be considered PII when combined:

• Full Name • Birthplace • Email Address • Telephone Number • Vehicle license plate number • Credit card numbers • Country, state, zip code or city of residence • Name of school attended or workplace • Financial Data • Physical Description	• Social Security Number (SSN) • Biometric records, photos, fingerprints • National identification number • Driver's license number • Age • Grades, salary or job position or history • Date of birth • Mother's maiden name • Statements made or attributed to the individual

C. RISKS

Given that data is any organization's most valuable asset, understanding the risks of mishandling PII can significantly prevent privacy breaches and the mishandling of participant information. When PII is illegally obtained, it is often used for financial gain and at the expense of the individual involved. Organizations collecting PII have an obligation to protect PII and are thus liable if it is ever compromised. It is the organization's responsibility to report any data losses and notify the individuals that may be affected. See Section III, Reporting a Data Breach, for more information.

II. DATA STORAGE, ACCESS, AND TRANSMISSION

A. STORAGE – DATA AT REST

1. Definition of terms

Antivirus	Software designed specifically to protect networks and devices against malware infection
Confidentiality	Keeping private data from improper or unauthorized disclosure
Data at rest	Refers to data that is stored on any media form which includes hard drives, external drives, USB flash drives, and backups
Encryption	Refers to the method of transforming confidential plain text into cipher text to protect it. An encryption algorithm combines plain text with other values called keys, or ciphers, so the data becomes unintelligible. Once encrypted, data can be stored or transmitted over unsecured lines. Decrypting data reverses the encryption process and makes the plain text available for further processing.
Firewall	Software/hardware that restricts the amount and type of network traffic going in and out of a network or device

Tailgating	The act of following a person closely behind in order to gain access to a secured area without showing credentials; often only takes a friendly smile to convince a person with access to hold the door open for someone without the proper credentials

2. Requirements

Securing data at rest is best accomplished with a combination of technical and operational controls. Devices containing PII must be physically secured, have firewall security measures enabled, with active and up to date anti-virus installed, access control implemented, and have data encryption enabled. All PII data will be housed in secured databases such as CalJOBS or SDWP hosted databases, servers, and file storage systems.

i. *Devices:*

All devices including desktops, laptops, and mobile devices must have complex passwords configured for access to the operating system as reference in **ATTACHMENT - PASSWORD POLICY**.

- Full Disk Encryption using AES-128 (or similar) must be implemented on any machine where PII data may reside
  - Encryption ensures that if in the even it is lost, misplaced, or stolen the PII data on the unit it is unreadable
- No PII data, at any time, shall be placed on unencrypted CD ROMs, external hard drives, thumb drives, or SD cards
- Mobile devices **shall not** be used to store PII data. Mobile devices are defined as:
  - Cell Phones
  - Tablets and iPads
  - Chrome Books
  - Personal Digital Assistants (PDAs)
- Only those explicitly authorized to maintain hardware used to store PII (computers, networks, applications) should have access to these devices

ii. *Physical Access Controls:*

- Any networking devices or physical hardware responsible for hosting data at rest must be within a locked cabinet and/or server room
- Only staff responsible for maintaining such hardware will have access to the locked cabinet and server room
- Limit physical access or entry to non-staff for areas that may contain PII
- A network firewall should be implemented to restrict the improper sharing of PII
- To ensure paper documents are secure at all times, desks must be locked when not in use if they contain PII
- Users must always log-off of desktops and laptops when not in use
- Refer to **ATTACHMENT – TRANSPORTING PHYSICAL PARTICIPANT FILES** to ensure that agents of SDWP and AJCC safeguard all confidential information while travelling from one facility/location to another during the course of their working day.

B. ACCESS – DATA IN USE

1. Definition of terms

Access	The ability or the means necessary to read, write, modify, or communicate data/information or otherwise make use of any system or data resource
Access Control	A method of restricting access to resources, allowing only approved users access. Includes identification, authentication, and authorization.
Authentication	Refers to the corroboration that a person or entity is who he/she/it claims to be
Authorization	Users are given access or permissions to access specific data and resources
Data in use	Data that is being modified using any application; resides in temporary memory
Least privilege	A technical control used to determine the rights and permissions assigned to each user; users should only have the minimum rights and permissions needed to perform their job
Need to Know	The concept that users are only granted access to the data necessary to perform their functions for the period of time required to complete the function

2. Requirements

- AJCC Operators and Subrecipients should determine the appropriate method and amount of PII to be collected from participants
    - The following topics should be taken into consideration:
        - What information should be collected
        - Why the information is collected
        - With whom the information will be shared
        - The intended use of the information
        - How the information will be secured
- Training is to be provided to each staff member, including volunteers and student interns, as well as any other individual who will likely to have contact with sensitive customer data and/or PII on the collection and handling of PII prior to being given access to participant data
- The level of access of each individual should be determined before the creation of their user account
- User accounts must be created based on “need to know” principle
- Accounts must be created for each user to claim an identity with a username (identification), prove that identity with a password (authentication), and access only the data they need to perform their job (authorization based on need to know)
- Only authorized users may access and use PII
- Users must use only devices, networks, applications and information for which they are authorized
- Sharing of usernames and passwords is prohibited
- Staff assigned mobile devices should be properly secured and their security status regularly verified

- Applications used to process PII must regularly be updated and patched
- Do not leave voice mail messages that include PII
- Users should never write down or record their passwords in unencrypted electronic files or documents
- Never leave your laptop (or any device with access to PII) unattended outside of the office

C. TRANSMISSION – DATA IN TRANSIT

1. Definition of terms

Data in transit	Any data that is being transmitted over a network
Phishing	When a malicious party sends a fraudulent email disguised as a legitimate email, often purporting to be from a trusted source. The message is meant to deceive the recipient into sharing personal or financial information or clicking on a link that installs malware.
Social Engineering	Involves the use of deception to manipulate individuals into divulging PII or company data that may be used for fraudulent purposes; can occur over the phone, in person, while surfing the internet, or via email

2. Requirements

- Any communication via email containing PII must be encrypted
- Networks should use encryption protocols; IPSec, SSH, SFTP
- Data Loss Prevention monitors should be in place and actively scanning emails and attachments that may contain PII on all outgoing traffic

iii. *Email Communication and Acceptable use*

Electronic email is pervasively used in almost all corners of work and life and is often the primary communication and awareness method within an organization. At the same time, misuse of technology and email can pose many personal and professional, as well as legal, privacy, and security risks, thus it is important for users to understand the appropriate use of electronic communications, and in particular:

1. Ensuring the confidentiality and security of customer data (PII)
2. Appropriate and acceptable use of computer technology and electronic communications
3. Expectations of sub recipients within the SDWP community

To protect yourself and participants, a combination of any two pieces of information that identify a participant (e.g. name and phone number) is considered PII and should never be sent in the body of an email message or as an attachment. If there is a business need to send PII over email, this information should be put into a document that can be encrypted and then sent as an attachment to an email message or a time-limited link. PII should **NEVER** be sent via email to external parties or entities (e.g. those with no contract or service agreement with SDWP), this includes screenshots from CalJOBS.

Note: Password protecting Microsoft files (such as Excel and Word):

There are a number of ways to protect your files with a password in order to add another layer of security, especially when sending documents over email. Password protecting a file or document means that the file is being encrypted so it cannot be opened or understood without a password. Encrypting PII information in transit protects from loss of confidentiality.

1. Open the file or document you want to encrypt
2. Go to “File” in the menu bar
3. Select the “Info” tab
4. Select “Protect Document” (Word), “Protect Workbook” (Excel), “Protect Presentation” (PowerPoint)
5. Click “Encrypt with Password”
6. The dialog box will provide a display to enter a password (up to 25 characters)
7. Enter the password two times to confirm following the password guidelines provided in this document.
8. Click “OK” then save the document
   When the document is sent via email the password will be required to open and read the document. The password should be sent in an email separate from the document so that someone who intercepts the email does not have access to the document and password simultaneously. You cannot open the document without the password and the password is useless without access to the document.

iv. *Risks of using email for sensitive data*

- Email is easy to falsify
- Email systems are backed up in many ways and deleting an email from both a recipient’s and a sender’s inbox does not insure the email has been permanently removed
- Employees do not have an expectation of privacy when communicating with their company email system. This is true for SDWP as well as anyone communicating with SDWP employees
- Email can be broadcast worldwide instantly and can be received by both intended and unintended recipients
- Recipients can forward any email message to other recipients without the original sender’s permission or knowledge

III. REPORTING A DATA BREACH

California law requires any organization/agency that maintains computerized data that includes PII to report any data, whether unencrypted or encrypted, that may have been acquired by an unauthorized person (California Civil Code s.1708.29 (a) and s.1729.82). Both from a legal and organizational accountability perspective, it is imperative that any suspected data breach or security incident be reported. Not every security incident result in actual data release, but every individual has the right and the responsibility to immediately report any actual or possible data breach or privacy violation, whether as a result of personal conduct or that of another worker, supervisor, officer or director. No concern is too small or unimportant. SDWP must be informed of a real or suspected disclosure. Therefore, the following steps must be taken upon the discovery of any potential or successful data breach

1. Complete **ATTACHMENT - NOTICE OF DATA BREACH: INCIDENT REPORT**
2. Submit the form to your program manager
3. Program manager will notify SDWP Help Desk <HelpDesk@workforce.org
4. An impact assessment will be conducted

5. Participants affected will be notified of breach by SDWP

SDWP Response to Security Incident Report
SDWP will take any and all reasonable steps to maintain the security of PII. When SDWP is notified of a security incident, and based upon the information received, SDWP will direct an investigation, determine what immediate action may needed, and develop a plan in collaboration with the sub-recipient to identify gaps and take corrective actions to prevent a future re-occurrence of a similar incident. If the investigation results in proof that PII was disclosed to unauthorized persons or systems, SDWP will notify the customer, and if necessary, federal and local authorities pursuant to applicable laws.

IV. ATTACHMENTS

AJCC Wi-Fi Usage Policy

Technical Support Between SDWP and AJCC Operator

AJCC E-Media Policy Acknowledgment Form

Password Policy

Transporting Physical Participant Files

Notice of Data Breach: Incident Report