SAN JOAQUIN COUNTY WORKNET
EMPLOYMENT AND ECONOMIC DEVELOPMENT DEPARTMENT
POLICIES AND PROCEDURES DIRECTIVE

DIRECTIVE NO.	EFFECTIVE DATE	APPLICABILITY	PAGE
24-21	March 1, 2025	Departmental	1 of 9
SUBJECT:	**INFORMATION SECURITY AND THE PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION**		

I. PURPOSE

The purpose of this directive is to provide guidance to staff and service providers on compliance with the requirements of acquiring, handling, transmitting and protecting personally identifiable information (PII), including the safe, secure, and acceptable use of computer equipment and systems, such as CalJOBS, for WIOA and National Farmworker Jobs Program (NFJP) activities administered by EEDD.

II. GENERAL INFORMATION

Recipients and subrecipients of WIOA Title I funds must have an internal control structure and written policies in place that provide safeguards to protect personally identifiable information (PII), records, contracts, grant funds, equipment, sensitive information, tangible items, and other information that is readily or easily exchanged in the open market, or that the Department or the recipient or subrecipient considers to be sensitive, consistent with applicable federal, state, and local privacy and confidentiality laws. WIOA service providers may have in their possession large quantities of PII relating to individual program participants. This information is generally found in participant enrollment applications, case files, both paper and electronic (such as the CalJOBS system). Service providers are required to take measures to mitigate the risks associated with the collection, storage, and dissemination of PII.

For NFJP, staff and service providers must protect personally identifiable information (PII) and other sensitive information in accordance with applicable federal, state, and local privacy and confidentiality requirements and the applicable

NFJP grant agreement. GPMS is the system of record for NFJP. Staff must make every effort to ensure that applicable NFJP information is accurate and appropriately protected in both CalJOBS and GPMS.

Any San Joaquin County or subrecipient employee using the County's computing and information resources is expected to act in a responsible manner by complying with all policies, relevant laws, and contractual agreements related to computers, networks, software, and computer information. This policy applies to anyone with access to San Joaquin County's computing and information resources and to all equipment that is owned or leased by the County.

As California's federally recognized system of record for tracking and reporting Workforce Innovation and Opportunity Act (WIOA) Title I, subtitle B, Title III Wagner-Peyser, Trade Adjustment Assistance (TAA), and Jobs for Veterans State Grant (JVSG) participants, CalJOBS provides a unified and streamlined intake and case management system that enables co-enrollment across programs, and consistent recording of data elements for reporting to the Department of Labor (DOL). The DOL requires state grantees to take measures to safeguard protected personally identifiable information (PII) and other sensitive information consistent with applicable federal and state laws regarding privacy and responsibility over confidentiality.

Definitions

For purposes of this policy, terms related to PII are defined as:

- **PII**: The Office of Management and Budget (OMB) defines PII as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

- **Sensitive Information**: Any unclassified information whose loss, misuse, or unauthorized access to, or modification of, could adversely affect the interest or the conduct of federal programs, or the privacy to which individuals are entitled under the Privacy Act.

- **Protected PII and non-sensitive PII**: The Department of Labor (DOL) has defined two types of PII, protected PII and non-sensitive PII. The differences between protected PII and non-sensitive PII are primarily based on an analysis regarding the "risk of harm" that could result from the release of the PII.

    1. *Protected PII* is information that if disclosed could result in harm to the individual whose name or identity is linked to that information. Examples of protected PII include, but are not limited to, 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, information regarding disability status, criminal records, financial information and computer passwords.

2. *Non-sensitive PII*, on the other hand, is information that if disclosed, by itself, could not reasonably be expected to result in personal harm. Essentially, it is stand-alone information that is not linked or closely associated with any protected or unprotected PII. Examples of non-sensitive PII include information such as first and last names,e-mail addresses, business addresses, business telephone numbers, general education credentials, gender, or race. However, depending on the circumstances, a combination of these items could potentially be categorized as protected or sensitive PII.

To ensure the safety of data stored in CalJOBS, the roles and the responsibilities related to CalJOBS staff user access are defined as:

- **Staff with access to CalJOBS**: This role includes anyone with a CalJOBS staff user account. Staff with access to CalJOBS must adhere to all requirements as outlined in the Vendor/Contractor Confidentiality Statement (Attachment 4).

- **Manager/Supervisor**: This role includes all managers, supervisors, project managers, and any other staff with oversight responsibilities for someone with a CalJOBS staff user account. Managers/Supervisors are responsible for ensuring staff complete annual ISPA training, sign the Vendor/Contractor Confidentiality Statement, and have a business need for CalJOBS access. Additionally, this role must ensure the data in CalJOBS is secure and being used by staff in accordance with this policy, and that access is updated and/or revoked as business needs change or the employee separates from their position. This role serves as the requestor for all CalJOBS staff user account requests.

- **CalJOBS Management Information System (MIS) Administrators**: This role is responsible for CalJOBS account creation, deactivation, and adjustment of staff access (privileges) for CalJOBS staff user accounts. This role reviews and processes CalJOBS System Access Request forms and Data Change Requests.

This PPD supercedes PPD D-10 The Handling And Protection Of Personally Identifiable Information (PII) (Rev 1), dated June 2, 2022.

References

- TEGL 39-11, Guidance on the Handling and Protection of Personally Identifiable Information (PII)
- WIOA Section 167, Migrant and Seasonal Farmworker Programs
- 20 CFR 683.220
- 20 CFR Part 685, National Farmworker Jobs Program
- WSD24-12, CalJOBS System Access
- WSD24-13, Local Area MIS Administrator and WSB CalJOBS SPOC Roles and Responsibilities

III. POLICY

It is the policy of the Employment and Economic Development Department that the handling and protection of confidential information will be conducted in accordance with the policies and procedures set forth in this directive. To ensure the confidentiality and security of PII, EEDD will not maintain protected PII in physical files. All PII must be stored electronically in secure, password-protected systems, such as CalJOBS, that comply with applicable data protection laws and organizational security protocols.

Physical storage of protected PII in paper files is prohibited to minimize the risk of unauthorized access, theft, or loss. In cases where physical records are absolutely necessary, they must be securely stored in locked, restricted-access locations and be handled with the utmost care to protect the privacy of individuals.

Effective information security is a team effort involving the participation and support of every EEDD employee and affiliate who deals with information and/or information systems. Every computer user must know this policy and conduct their activities in compliance with it. In accordance with San Joaquin County Countywide Information Security Policies, Internet/Intranet/Extranet-related systems, including, but not limited to, computer equipment, software, operating systems, storage media, network accounts providing electronic mail, web browsing, and file transfer protocol, are the property of San Joaquin County. These systems will be used only for authorized County business purposes in serving the interests of the organization and the public in the course of normal operations.

EEDD requires staff, subcontractors, and others under department oversight to agree in writing to protect information assets and to comply with EDD information security requirements. As CalJOBS houses PII, users must ensure it remains secure at all times. Staff with access to information resources must read, understand, and comply with the San Joaquin County Information Security Handbook (Attachment 1). Appropriate use is summarized in Appropriate Use of County Resources (Attachment 2).

To ensure staff knowledge remains current, EEDD staff must complete Information Security and Privacy Awareness (ISPA) training annually. This is a mandatory training for all San Joaquin County employees regardless of status. This includes full-time, part-time, temporary and seasonal staff. In accordance with WSD24-12, ISPA training must be completed prior to receiving a CalJOBS account. It must be updated annually to maintain a CalJOBS account.
This policy is based on EEDD interpretation of WIOA law and subsequent federal, state, and local laws, regulations, and policies and applies to all WIOA and non-WIOA programs administered by EEDD.

IV. PROCEDURE

Federal law, and OMB Guidance policies require that PII and other sensitive information be protected. To ensure compliance with federal law and regulations, staff must secure the storage and transmission of PII and sensitive data developed, obtained, or otherwise associated with WIOA and NFJP funds.

In addition to the requirement above, all grantees must also comply with all of the following:

- All staff must complete Information Security and Privacy Awareness (ISPA) training when hired and subsequent training annually. The San Joaquin County Information Services Division (ISD) provides ISPA training to all county employees on an annual basis. When an employee receives access to the training from ISD, they must complete it within 30 days. New employees must complete the training within 30 days of their hire date.

- To ensure that PII is not transmitted to unauthorized users, all data at rest and data in motion is encrypted to avoid any potential breach. In the event of a breach, security policies and measures for involving the San Joaquin County security officer have been established providing protocols to follow for notification and correction.

- SSL encryption has been instituted on all websites that move PII data.

- EEDD staff and service providers 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. Grantees must maintain such PII in accordance with this policy.

- EEDD staff and service providers will ensure that any PII used during the performance of their grant has been obtained in conformity with this

policy and applicable federal and state laws governing the confidentiality of information.

- EEDD staff and service providers further acknowledge that all PII data obtained through their WIOA grant will be stored in an area that is physically safe from access by unauthorized persons at all times and the data will be processed using grantee issued equipment, managed information technology services, and designated locations approved by the administrative entity. Accessing, processing, and storing of WIOA grant PII data on personally owned equipment, at off-site locations e.g., employee's home, is strictly prohibited.

- EEDD staff and service provider employees and other personnel who will have 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.

- EEDD staff and service providers must have policies and procedures in place under which grantee employees 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.

- EEDD staff and service providers must not extract information from data supplied for any purpose not stated in the grant agreement.

- Access to any PII created by the WIOA grant must be restricted to only those employees of the grant recipient who need it in their official capacity to perform duties in connection with the scope of work in the grant agreement.

- 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 or any other means. Unencrypted emails must not include PII data. Data may be downloaded to, or maintained on, mobile or portable devices only if the data are encrypted using NIST validated software products based on FIPS 140-2 encryption.

Protected PII is the most sensitive information encountered in the course of grant work, and it is important that it stays protected. AJCC staff and service providers are required to protect PII when transmitting information, but are also required to

protect PII and sensitive information when collecting, storing and/or disposing of information as well. Outlined below are procedures intended to protect PII:

- Before collecting PII or sensitive information from participants, have participants sign releases acknowledging the use of PII for grant purposes only.

- Use unique identifiers, such as a WIOA application number or CalJOBS State ID for participant tracking instead of SSNs or even truncated SSNs. While SSNs may initially be required for performance tracking purposes, a unique identifier will also be linked to each individual record. Once the SSN is entered where required, the unique identifier must be used in place of the SSN for tracking purposes.

- Use appropriate methods for destroying sensitive PII in paper files (i.e., shredding or using a burn bag) and securely deleting sensitive electronic PII.

- Do not leave records containing PII open and unattended.

- Immediately report any breach or suspected breach of PII to EEDD Administrative Entity Staff, who will report it to ETA Information Security at ETA.CSIRT@dol.gov, (202) 693-3444, and follow any instructions received from officials of the Department of Labor.

To ensure the security of information stored in CalJOBs, in accordance with WSD24-12, all staff are required to complete the following before a request for CalJOBS access can be submitted:

1. Complete annual ISPA training. The last date completed cannot exceed 365 days from the CalJOBS staff user account request date.

2. Sign the Vendor/Contractor Confidentiality Statement. The last date completed cannot exceed 365 days from the CalJOBS staff user account request date.

Once the above requirements are met, the requestor must submit a completed CalJOBS System Access Request Form (Attachment 3) and a signed Vendor/Contractor Confidentiality Statement (Attachment 4) to their supervisor who will provide it to the designated MIS Administrator who will create the CalJOBS account and upload the required documentation to CalJOBS.

Once the staff user account is created, the CalJOBS username and temporary password will be provided to the staff with a carbon copy (cc) to the requestor. The first time the staff logs into CalJOBS with their username and temporary password,

they will be immediately prompted to establish a new password. Staff must be reminded that their username and password are to be kept confidential.

If staff needs their CalJOBS staff user account reset, the requestor must submit a new CalJOBS System Access Request Form (Attachment 1) to their supervisor, who will provide it to the designated MIS Administrator to process the request. Once the staff user account is reset, the CalJOBS username and temporary password is provided to the staff with a cc to the requestor. The temporary password expires after 24 hours. The first time the staff logs into CalJOBS with their username and temporary password, they are immediately prompted to establish a new password. Staff must be reminded that their username and password are to be kept confidential.

System access is provided to staff based on their primary job function. Staff may be asked to perform additional duties within CalJOBS other than their daily tasks which may require access to certain areas of CalJOBS not already granted. If staff require additional access (privileges) within CalJOBS, the requestor must submit a new CalJOBS System Access Request Form (Attachment 1) to their supervisor, who will provide it to the designated MIS Administrator to review process the request, if access can be granted. If an access request is denied, a reason for denial will be provided.

To maintain the security of the data housed within CalJOBS, a staff's CalJOBS account must be revoked prior to, or at the time of their separation from the organization, or when there is no longer a business need for the access. To deactivate an account, the requestor must submit a CalJOBS System Access Request Form (Attachment 1) to the designated MIS Administratio. Requests to deactivate a staff user account should be submitted with as much notice as possible to ensure the request is processed prior to the staff no longer needing access.

Notification of Subrecipients and Partners

Subrecipients and partners of the EEDD must be informed of the EEDD's information security policies and procedures when entering into an agreement or MOU. Subrecipients or partners must follow EEDD information security policies or have their own information security policy approved by the EEDD.

Employee Acknowledgement

Upon hire, all EEDD employees must acknowledge that that they have received a copy of this policy by completing and signing the Employee Acknowledgement of the Policy and Procedures Directive on the Handling and Protection of Personally Identifiable Information (PII) (Attachment 5). Subrecipient and partner staff must also sign and complete the Employee Acknowledgement or comply with their own

information security policy approved by the EEDD upon entering into an agreement or MOU.

V. QUESTIONS REGARDING THIS DIRECTIVE

May be referred to the Executive Director of EEDD via Managers or designee.

VI. UPDATE RESPONSIBILITY

The Executive Director of EEDD and/or designee will be responsible for updating this directive, as appropriate.

VII. APPROVED

Patricia Virgen

PATRICIA VIRGEN
EXECUTIVE DIRECTOR

PV:jl

Attachment 1: San Joaquin County Information Security Handbook
Attachment 2: Appropriate Use of County Resources
Attachment 3: CalJOBS System Access Request Form
Attachment 4: Vendor/Contractor Confidentiality Statement
Attachment 5: Employee Acknowledgement of the Policy and Procedures Directive on the Handling and Protection of Personally Identifiable Information (PII)

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. This program is substantially funded by federal funding. For more information go to: www.sjcworknet.org/WIOAresources.asp

San Joaquin County

Information Security Handbook

August 31, 2009

This Handbook Describes What You Need To Know To Be An Active Participant In

THE SAN JOAQUIN COUNTY INFORMATION SECURITY PROGRAM

- Discover How To Make A Difference -

Table of Contents

Forward 4
Information Security Goals 5
What are the Threats? 6
Policies and Controls 8
Public and Private Information 9
Legal Responsibilities 10
Handling Contacts With People 11
Disposing of Information Properly 12
Protecting Information in the Work Area 13
Personal/Private owned Equipment 14
Passwords 15
Protecting County Equipment 17
Away From the Office 17
Software 18
Wireless Devices 19
Backing Up Information 19
Viruses, Trojans and Malware 20
Information Security Incidents 21
The Most Valuable Asset 22

Forward

San Joaquin County handles sensitive and confidential information daily. As employees of San Joaquin County, we have been entrusted with County information. With this trust comes the responsibility and obligation to ensure that information is used only for its intended business purpose. The information we use every day must be protected. Whether we work with paper records, a computer, or spend most of our day on the phone.

Anyone given the privilege of using San Joaquin County's computing and information resources is expected to act in a responsible manner by complying with all policies, relevant laws, and contractual agreements related to computers, networks, software, and computer information. To assist in understanding the policies and expectations of the County, this document has been developed. This document highlights existing County Information Security policies.

Ensure that you are aware of all your responsibilities. Read the **Information *Security Program*** and ***Information Security Policies*** on the County Intranet at http://sjchome.

When using County computing and information resources, a good general rule to follow is:

If it isn't County business, don't go there.

INFORMATION SECURITY IS OUR RESPONSIBILITY

Information Security Goals

Information is a valuable asset that needs to be protected from loss, unauthorized changes, and unauthorized disclosure.

The goal of Information Security is to ensure the confidentiality, integrity, and availability of information through safeguards.

"Confidentiality" – Assurance that information will not be disclosed to unauthorized individuals or processes. Disclosures can be from personal conversations, email, printed documents, unprotected data or other sources. Information must be classified properly and appropriate safeguards put in place.

"Integrity" – Assurance that information has not been altered or destroyed in an unauthorized manner. Information with integrity can be trusted and relied upon.

"Availability" – Assurance that systems and information are accessible and useable by those who need them.

Information appears in many forms.

Here are some examples:

CONVERSATION	FAX	MICROFILM
TELEPHONE	DISKETTES	CD'S
PAPER REPORTS	EMAIL	SCHEDULES CALENDARS
LETTERS	MEMOS	COMPUTER DISPLAYS

AND

"THE INTERNET"

What are the Threats?

Every day, the County is faced with threats that can often result in stolen or altered information. Unauthorized people could maliciously delete, or browse information, whether or not it is confidential or sensitive. At risk is the integrity of critical files and systems. The impact can have a devastating effect on the County. These threats take many forms.

Examples of Threats:

- Viruses
- Worms
- Hoaxes
- Wireless Attacks
- Identity Theft
- Hackers
- Phishing
- Social Engineering Attacks
- Instant Messaging
- Physical Security Flaws
- Spam
- Spyware

Impact of Malicious Actions

The impact of malicious actions can be devastating.

- Personal information loss can result in identity theft
- Employees could face disciplinary actions
- Corrupted information could cost time and money to recreate
- The County's reputation and credibility could be damaged from bad publicity from media coverage and news reports
- There could be a loss of trust by employees and the public
- Giving out private information could cause costly legal actions to be brought against the County
- Management could make a bad decision based upon incorrect information

More than ever, it is important to be AWARE of what can be done to help minimize these risks.

Policies and Controls

Policies are needed to ensure that each person is accountable for his or her actions. Controls built from County policy protect the honest user from unfair suspicion. Without accountability, all are equally suspect when something bad happens.

Problems with information are usually caused by honest errors or omissions. Controls help prevent errors, identify those who need help, and limit the damage their mistakes cause.

Lack of policies and controls results in ineffective security.

Policy and controls example:

Internet access provides a good example of why policies and controls are needed. The Internet constantly challenges us with security risks such as viruses and hackers, but the County needs to access the Internet for day-to-day tasks. Even if all Internet security risks were eliminated, there are still issues with the vast content of information that is not business related. If access to the Internet content is not controlled, staff could accidentally enter a web site that contains pornography or gambling. This could easily offend the computer operator or anyone that can see what is being displayed on the screen. If the computer is in a public area, children could be exposed to adult content. To address these concerns, a countywide web filtering policy and software standard were established. All County access to the Internet must be done through the standard web filtering system. This provides department heads with the ability to control Internet access to those sites that support business requirements.

The *Information Security Program* and *Information Security Policies* can be found on the County Intranet at ***http://sjchome***.

Public and Private Information

Even though we are a local government agency, we have a responsibility to protect the privacy of our citizens and employees, and to ensure that government continues to serve our community without costly interruptions or loss of data.

Some of the information that we are entrusted with is not necessarily public information. Examples of private information would be credit information, social security numbers of employees or customers and most law enforcement information.

There are federal laws that protect a person's right to privacy and prohibit unauthorized computer access and violation of copyright, patents, and trade secrets. Violation of these laws can result in litigations.

Legal Responsibilities

The County is legally obliged to protect information furnished by employees or customers and is accountable for correct and appropriate use. Inaccurate information can lead to legal issues.

The laws such as the 1987 Computer Security Act, the Health Insurance Portability and Accountability Act (HIPAA), and the Sarbanes–Oxley Act (2002) were brought in to safeguard privacy and regulate information dissemination.

California laws, such as “California Penal Code 502” affords protection to individuals, businesses, and governmental agencies from tampering, interference, damage, and unauthorized access to lawfully created computers, computer systems, and computer data.

Handling Contacts With People

Social Engineering

"*Social Engineering*" is a term indicating the method in which people are manipulated, rather than machines, to gather information to bypass or breach the security systems of an enterprise. It is probably the greatest security risk that we face in protecting our information from theft and misuse, even greater than direct hacking of our systems.

How do you guard against Social Engineering?

- Don't allow yourself to be pressured or hurried by someone.
- Follow security procedures and don't take short-cuts.
- Ask for photo identification (two if possible) of visitors and then verify it.
- Escort visitors at all times while in your work areas (even telephone technicians).
- When required in your work areas, issue appropriate guest name tags and document or log guest activities per your area's security policy.
- Don't volunteer unnecessary or unrelated information.
- Don't respond to e-mails or phone calls asking you to "update information for their records" (this includes software, computer or telephone systems that we use at the County).
- When asked to complete a survey or questionnaire, ask your supervisor whether this is acceptable.
- Do not provide lists of employees or telephone numbers without proper authority.

Always notify your supervisor if someone seems suspicious or out of place.

Disposing of Information Properly

What Do I Do with Paper or Computer Media That is No Longer Needed?

Check with your manager or supervisor about the approved method for disposing of documents or any kind of information.

Some of the methods that may be used are:

- Confidential documents should be shredded. Your department may ask you to place documents in a special collection area for disposal. Ask your manager or supervisor what procedure to follow.
- When disposing of old media such as floppy diskettes, tapes and hard drives, erase all information with one of the County's certified degaussers. Use County certified software to erase hard drives that will be reused.
- When disposing of CD's, cut or break them in half before putting them in the trash.

Protecting Information in the Work Area

We become careless about the information in our work area because we have authorized access to it. It's Important to prevent access by:

- Locking sensitive documents in a cabinet or drawer
- Clearing our desk of sensitive papers at the end of the day
- Keeping keys under control (don't loan them to anyone)
- Establishing a need to know before discussing work with others
- Labeling sensitive documents appropriately
- Challenging unfamiliar / unauthorized visitors

Protecting Your Computer:

- Make sure that anyone you see using a computer in your area is authorized to do so.
- When sensitive information is on the screen, be sure no one else can see it.
- Protect your password.
- Make sure a password protected screen saver has been installed.
- Unattended or inactive computers should be 'locked' or logged off within a time no longer than 15 minutes.

Who Really Owns the Computer that I Use?

Your equipment is owned by the County. It is your responsibility to protect the equipment and software from misuse. Be mindful that loading un-authorized software, toolbars, music players and other utilities may cause your computer to slow down or stop working altogether.

Personal/Private owned Equipment

Can I use my personally owned computer at the County?

You cannot connect any personally or privately owned computer, cell phone or other portable media device directly to any portion of the County's network.

This includes but is not limited to personal computers, PDAs, Blackberrys, Cell phones, Smart phones, USB drives, etc.

With department head approval, personally/privately owned computers, cell phones or other portable media devices may be indirectly connected to the County network. Indirect connection may be through approved VPN or OWA access points only. Any connection must comply with County Information Security Policy and must be properly licensed for those systems being accessed.

Passwords

Why Should I Protect My Password?

Your password gives you access to County computer systems and it is your responsibility to protect it.

To protect your password:

- Change your password at least every 90 days.
- Change your password immediately if it becomes known to others.
- Choose "hard to guess" passwords.
- Log off after each use. Never leave an active session unattended. You are responsible for any activity on that computer.

How Do I Choose A New Password?

The whole idea of a password is to keep someone else from accessing your computer. The password you choose should be easy to remember and hard to guess.

Passwords To Avoid:

- Your name, nickname, initials
- Your children's names or nicknames
- Your user ID code
- Dates, especially those that appear on your driver's license or on a calendar you carry in your wallet or purse
- The license number of your car(s)
- Consecutive keys on a keyboard, e. g. QWERTY or FGHJKL
- Any part of your Social Security Number
- Words that appear in a dictionary.

Passwords (continued)

Here Are Some Suggestions for Choosing a Good Password:

- Combine letters and numbers such as the name and birth date of a relative or friend, e. g. LISA1055
- Take the first or last letter from each word of a phrase, e. g. EDESOEFT (wE holD thesE truthS tO bE selF evidenT) and add a number to the end “EDESOEFT1”.
- Remove all vowels from a common word or words, e. g. TPSCRT (ToP SeCReT)
- Make it as long as possible
- Use a non-English word

What Are Pass-Phrases?

A pass-phrase is like a password only longer, easier to remember and harder to guess. A simple pass-phrase might be the words of your favorite song or a line from a movie. Note that spaces and special characters are allowed and included in a pass-phrase. Here are some examples of simple pass-phrases:

“Can’t Touch This!” (17 character pass-phrase)

“What we've got here is failure to communicate” (45 character pass-phrase)

A stronger pass-phrase example would be to use the same words but substitute some of the characters with special characters (a-z, A-Z, 0-9, !@#$%^&*()) which dramatically increases the time needed to crack a password e.g. “C@n’t-T0uch-Th|s!”

Just a reminder, DON'T use any passwords provided above. A lot of people will be reading this handbook.

DON'T SHARE YOUR PASSWORD WITH ANYONE!

Protecting County Equipment

Away From the Office

Personal computers may be stolen or damaged when they are removed from the office. The same rules apply to County equipment when using it at work or away from the office.

When removing equipment from the office, be sure to:

- Get written approval from your manager or supervisor.
- Use extra care in handling the equipment. It is very fragile.
- Use extra care to protect the equipment from loss or theft.
- Always keep it in sight when traveling.
- Lock up equipment when not in use
- Do not leave equipment in hotel rooms – check computer equipment with hotel front desk if possible
- Don’t leave equipment in vehicles

Software

What Are the Rules?

Installing software, including the downloading of any software from the Internet, can only be done with the approval of your department.

This includes freeware, upgrades to existing software, shareware, demonstration software and trial/evaluation software.

No one can bring computer equipment and / or software to the County without permission from management.

Can I Make a Copy of County Owned Software to Use On My Home Computer?

When in doubt, don't copy!

Here are some guidelines for copying software:

- Some agreements between the County and software vendors may allow copying of software if the use is business related.
- Obtain your managers/supervisor's written approval before copying any software.
- Although the County may have purchased the software, what we really buy with these packages is a license to use the software on one machine.
- Unauthorized copying of software is a violation of U. S. Copyright Law. It is critical that you check the terms of the license to make sure you are not violating the agreement with the vendor.
- Misuse of software could expose you to lawsuits by the software vendor.
- If you are borrowing the original software, use great care to protect it from damage.

Wireless Devices

Can I Connect Wireless Devices to the Network?

You must have permission to connect any wireless device to a County network. Deployment of ANY wireless device or access point without permission is not allowed and is subject to disciplinary action.

Backing Up Information

"YES" you Should Backup Information.

Data and other forms of important information should be backed up. Back up information is needed when something happens to the original copy.

Remember the purpose of an extra copy is to replace the main copy if something happens to it.

Information should be backed up if:

- It would take considerable time and money to recreate it
- You could not recreate it because the original source is gone

Being prepared is part of disaster recovery.

- You may need to send an extra copy off site as a protection against an office disaster.
- Test your back-up copy to ensure it will actually restore the information.

Viruses, Trojans and Malware

How Can I Protect My Computer from Viruses?

- Make sure that you have current antivirus installed on your computer.
- Never disable the anti-virus software.
- Do not click on unknown Web links found in e-mail messages or links found on unfamiliar Web sites.
- Do not open attachments unless you are expecting information from someone. If you receive an unexpected attachment, call to verify that it is legitimate before you open it.
- Don't share diskettes, CDs or files that have not been scanned for viruses.

E-mail Hoaxes

E-mail hoaxes are seemingly credible warnings, reports or stories that sound very believable and truthful, but are un-verifiable and most often a lie. Do not forward this type of email to other staff.

Spyware

Spyware is a type of malware that is installed on computers and collects information about users without their knowledge. Sometimes, key logger spyware is installed to secretly monitor other users.

Avoiding downloads of freeware or shareware will decrease the possibility of spyware being installed on your computer.

Remember the general rule:

If it isn't County business, don't go there.

Information Security Incidents

A security incident, threat, or breach is a situation where the safety of a physical environment or its contents is endangered.

Identifying a potential security breach requires you to be aware of your surroundings, knowing what is normal and what is out of the ordinary.

Combining vigilance, common sense, and knowledge of your organizational policies should enable you to recognize possible security incidents.

Information security problems or suspected problems should be reported immediately to your supervisor.

Examples:

- Compromise of integrity (virus infects a program)
- Discovery of serious system vulnerability
- Denial of service (attacker disables a system)
- Misuse (intruder or insider makes unauthorized use of
- an account)
- Damage (virus destroys data)
- Intrusions (intruder penetrates system security)

If you suspect a crime is being committed, make sure that the appropriate law enforcement agency (e.g., Police) is notified. This includes email threats against personal life or safety.

The Most Valuable Asset

IT SEEMS LIKE THE COUNTY IS REALLY SERIOUS ABOUT INFORMATION

BUT, AREN'T PEOPLE IMPORTANT, TOO?

Employees are the County's most valuable asset. The security and safety of all employees is important. Familiarize yourself with County safety programs and emergency procedures.

Knowing what to do in an emergency could protect
The most valuable asset — **YOU**!

As you can see, there are a lot of things which you can do to protect information in all its forms. The suggestions in this booklet are for you to use every day to make County information and assets secure.

Any Questions?

If you are unsure about what to do:

Review the County Information Security Policies. A link to these documents is on the front page of the County Intranet web site at: **http://sjchome**

If you cannot find the answer there, ask your *supervisor*, *Departmental Information Security Representative* or *County Information Security Officer* at 209-468-8426.

WHAT IS THE KEY TO INFORMATION SECURITY?

All of us are the key to information security.
Remember to BE AWARE!

Attachment 2

VEHICLES

County-owned automobiles shall be used only to conduct County business. No County employee shall use, or permit the use of, any County-owned automobile for any purpose other than County business.

If you have any questions regarding the material in this document, please contact your supervisor / manager.

The following sections of the Administrative Manual were referenced in the development of this document:

- *Data Processing Services (1500)*
- *Telephone System (3300)*
- *Vehicle Usage – County and Private (3700)*

The Administrative Manual and Information Security policies can be referenced on the County Intranet at *http://sjchome*.

This document was produced by Information Systems Division on behalf of the County Administrator.

SAN JOAQUIN COUNTY

Appropriate Use of County Resources

JANUARY 2021

Appropriate Use of County Resources

It is the intent of San Joaquin County to provide its employees with tools that assist in the delivery of goods and services to the people of the County. It is the responsibility of each County employee to use these tools in an appropriate manner. To assist County employees in understanding the policies and expectations of the County, this document has been developed. This document highlights existing County policy regarding appropriate use of County resources. For greater detail, please refer to the Administrative Manual (Sections 1500, 3300 and 3700) available in each County office. Information Security policies can be referenced via a link on the County Intranet at *http://sjchome*

First and foremost, all resources provided by the County must be used only for County business. Employees shall not use, or permit to be used, any County resource for a purpose other than that necessary for County business. Each employee has an obligation to use the tools provided in a manner that is consistent with the public trust. Equipment must be used in a manner that does not jeopardize security, confidentiality, or place the County in a litigious position. Use of the equipment must not violate any law regarding privacy, public record or copyright.

An overview of the most common County resources and associated policy follows:

COMMUNICATION DEVICES

The County provides its employees with a wide variety of communication tools. These tools are provided for the sole purpose of conducting County business. Employees should be careful not to disclose confidential or proprietary County information. It is essential that these tools not be used to transmit, receive or store any communication that is discriminatory, or harassing in nature, or that could be perceived as obscene. Communication tools provided by the County include:

TELEPHONES

Telephones are provided for the purpose of completing County business. Employees will be required to reimburse the County for unauthorized calls that result in a cost to the County.

FACSIMILE MACHINES

All communications sent or received via FAX machines must be for County business only.

VOICE MAIL

The greetings that a caller hears form their first impressions of the employee and the County. Key points to remember:

- *Make sure the greeting is business-like and courteous*
- *Give callers instructions on how to reach a live person*
- *Update your voice message when you are out of the office for an extended period of time*

COMPUTERS / COMPUTER TECHNOLOGY

The purpose of the County's computer technology system is to share information and improve the way service is provided to the public and its employees. As this technology provides connectivity, the actions of one person can impact the integrity and security of a network used by many. Any employee given the privilege of using San Joaquin County's computing and information resources is expected to act in a responsible manner by complying with all policies, relevant laws, and contractual agreements related to computers, networks, software and computer information. As the County's use of the Wide Area Network (WAN) and the Intranet expands, more County employees are using computer technology to share information, making a secure environment very important. In the future, the County Intranet will continue to evolve where staff, with proper access rights, can obtain a wide variety of information, such as employee and benefits information.

Key issues to remember when using County computer equipment:

- *The equipment is provided for the purpose of facilitating County business*
- *All software must be installed, regularly updated and used in accordance with the associated copyright provisions*
- *Anti-virus software must be installed, regularly updated and running on all computers*
- *Any communications, access to County resources should use our VPN for the sole purpose of enabling County business.*
- *Privacy, security, integrity and confidentiality of the information should be maintained at all time*
- *Do not leave your computer on and unattended – especially in areas providing public access*
- *Change your password at least every 90 days*
- *All computer information created using County computer resources is the property of the County*
- *Using a modem to connect to an external source can jeopardize the security of County information*
- *All access to the Internet made via County computers can be monitored by the County*
- *All Internet, Intranet, collaborative tool usage (Microsoft Teams) and electronic mail messages created, sent or retrieved over the County's network are not private. All such messages can be monitored and audited for content*
- *Transmitting, retrieving or storing any communication of a discriminatory or harassing nature is prohibited by County Policy*
- *Transmitting, retrieving or storing any communication or image that is abusive, profane or offensive is prohibited by County Policy*

CalJOBS[SM] System Access Request Form

Request Type

Does the staff currently have or has ever had a CalJOBS staff account?

If yes, CalJOBS username:

Indicate the action needed for this staff account:

If inactivating, provide date and time to inactivate account: (last date/time access is needed)

Staff Information

Organization Type: If Other, provide description:

Subgrantee Code[1]: ARU[2]:

First Name: Last Name:

Agency Name: Job Title:

Office Zip Code: Phone Number: Email[3]:

Primary Office Information

Local Workforce Development Area Region:

Default Office:

Other Office Locations:

Does the staff need supervisor level access to the offices above?

Additional access needed (select all that apply):

☐ DVOP ☐ LVER ☐ TAA ☐ ETPL ☐ DOC (REO Corrections) ☐ NFJP

Data Security Requirements

Staff has a business need for CalJOBS access? ☐ Yes ☐ No

Employee or Contractor Confidentiality Agreement Signed: ☐ Yes ☐ No Most Recent Date:

Information Security and Privacy Awareness Training (or equivalent) Completed: ☐ Yes ☐ No
Most Recent Date:

Requestor Information

Name: Job Title:

Email: Phone Number:

Signature: Date:

Account Creator

Name: Job Title:

Signature: Date:

Return completed and signed form to CalJOBS System Access Coordinator

[1] Only applies to Local Workforce Development Area and Community-based Organization staff.
[2] Only applies to Workforce Services Branch staff.
[3] Email must be an organization-provided email (no personal email addresses allowed).

ATTACHMENT E-1

(Standard/Interagency Agreement)

VENDOR/CONTRACTOR CONFIDENTIALITY STATEMENT

Information resources maintained by the State of California Employment Development Department (EDD) and provided to you may be confidential or sensitive. Confidential and sensitive information are not open to the public and require special precautions to protect it from wrongful access, use, disclosure, modification, and destruction. The EDD strictly enforces information security. If you violate these provisions, you may be subject to administrative, civil, and/or criminal action.

I, _____ an employee of _____

PRINT YOUR NAME — PRINT YOUR EMPLOYER'S NAME

hereby acknowledge that the confidential and/or sensitive records of the Employment Development Department are subject to strict confidentiality requirements imposed by state and federal law including, but not limited to, Unemployment Insurance Code (UIC) §§ 1094, 2111 and 2714; California Civil Code (CC) § 1798 et seq.; California Penal Code (PC) § 502; 5 United States Code (U.S.C.) § 552a; 18 U.S.C. § 1905; and 20 Code of Federal Regulations (C.F.R.) § 603 et seq.

- I acknowledge that the Contract's Confidentiality and Data Security Monitor reviewed with me the confidentiality and security requirements, policies, and administrative processes of my organization and that of the EDD.
- I acknowledge responsibility for knowing the classification of the EDD information I work with and agree to refer questions about the classification of the EDD information (public, sensitive, confidential, Federal Tax Information) to the Contract's Data Security Monitor.
- I acknowledge privacy, confidentiality, and data security laws apply to the EDD information I have been granted access to by my employer, including, but not limited to, UIC §§ 1094, 2111, and 2714; Government Code § 15619; CC § 1798.53; and PC § 502.
- I acknowledge that wrongful access, inspection, use, modification, or disclosure of confidential information may be punishable as a crime and/or result in civil action taken against me, and/or fines and penalties resulting from criminal prosecution or civil lawsuits, and/or termination of contract.
- I acknowledge that wrongful access, inspection, use, modification, or disclosure of confidential information for personal gain, curiosity, or any non-business related reason is a crime under state and federal laws.
- I acknowledge that wrongful access, inspection, use, modification, or disclosure of confidential information is grounds for immediate termination of my employer's Contract with the EDD.
- I acknowledge that I understand the penalty provisions of Internal Revenue Code (26 U.S.C. §§ 7431, 7213, and 7213A).
- I acknowledge that upon discovering a possible improper inspection or disclosure of Federal Tax Information (FTI), including breaches and security incidents, I must follow the proper incident reporting requirements issued by the EDD. If I think there is a mishandling of information I will contact my EDD contract monitor and contact the EDD Information Security Office to ensure the Office of Safeguards and the Treasury Inspector General for Tax Administration are notified of a possible issue involving FTI.
- I hereby agree to protect the EDD's information on either paper or electronic form in the following ways:
  - Access, inspect, use, disclose, modify, remove or destroy information only for the purpose of performing official duties
  - Never access, inspect, use, disclose, modify, remove, or destroy information for curiosity, personal gain, or any non-EDD and/or my organization's business related reason
  - Never post the EDD and/or other agency/entity confidential and proprietary information to social media, networking or other public websites
  - Secure confidential information in approved locations and destroy confidential information by approved methods
  - Never use personal devices, including but not limited to, laptops, cameras, video recorders, portable electronic devices containing cameras such as, iPads, tablets and mobile smartphones, in the workplace to capture or record confidential information, including that which appears in the background in work areas
  - Only use authorized state business devices to capture or record confidential information when there is a business need and meets the EDD's guidelines
  - Never remove personal, sensitive, or confidential information from my work site without authorization
  - Follow encryption requirements for all personal, sensitive, or confidential information in any portable device or media

---

CERTIFICATION

I expressly consent to the monitoring of my access to computer-based sensitive, personal, or confidential information by the Franchise Tax Board, the Employment Development Department, the California Department of Tax and Fee Administration, the Department of Motor Vehicles, the Board of Equalization, and any other State agency designated by them.

My signature verifies that I read and agree to comply with the state and federal laws listed on this form. I further understand that failure to comply with these laws may result in my being barred from accessing the EDD information or other information provided by the EDD and could result in criminal prosecution.

CONTRACTOR NAME (PRINT)	EMPLOYER (PRINT COMPANY NAME)
CONTRACTOR SIGNATURE	DATE

ATTACHMENT E-1
(Standard/Interagency Agreement)

Vendor/Contractor Confidentiality Statement Completion Instructions

The Vendor/Contractor Confidentiality Statement informs all EDD vendors and contractors of their information security responsibilities.

NOTE: Failure to sign the Vendor/Contractor Confidentiality Statement does not exempt the vendor/contractor or non-EDD staff from their responsibility to ensure that the EDD's confidential information assets are protected.

Additional information is available upon request. Please see:

- "Vendor/Contractor Fact Sheet"

Employee Acknowledgement of the San Joaquin County Employment and Economic Development Department Policy and Procedure Directive:
The Handling and Protection of Personally Identifiable Information (PII)

By signing below, I acknowledge that I have received a copy of the above referenced Policy and Procedure Directive regarding the Handling and Protection of Personally Identifiable Information. I understand that access to sensitive/confidential/proprietary/private data requires the established safeguards to protect the information; and that there are civil and criminal sanctions for non-compliance with such safeguards contained in Federal and state laws.

_____
Print Name

_____
Title

_____
Agency

_____
Signature

_____
Date