

Memorandum of Understanding

Between
The State of California Employment Development Department (EDD)
and
California Statewide Automated Welfare System (CalSAWS)

This Memorandum of Understanding (MOU) is entered into by and between the Employment Development Department, hereinafter referred to as EDD, and the California Statewide Automated Welfare System, hereinafter referred to as SAWS.

I. PURPOSE

The purpose of this MOU is to establish a non-monetary cooperative agreement which will allow EDD access to the SAWS database to review and retrieve recipient benefit information necessary for the Work Opportunity Tax Credit (WOTC) program to verify and determine eligibility and issue Work Opportunity Tax Credit certifications.

II. LEGAL AUTHORITY

42 U.S.C. §1320b-7 Subsection (a)(5)(A) EDD, as California's State Workforce Agency (SWA) administering WOTC, to negotiate formal cooperative agreements with state and local agencies to participate as appropriate in the program to enhance and properly achieve the mission of EDD's services.

III. TERM OF MOU

The term of this MOU is May 1, 2025, through December 31, 2026, unless the Federal Government extends the duration of the WOTC program, in which event this MOU will remain in force unless otherwise modified or terminated by either party.

IV. WOTC OBJECTIVES

The purpose of the WOTC program is to provide a federal tax incentive to employers to hire and employ individuals from the following targeted groups:

- Qualified Short Term Temporary Assistance for Needy Families (TANF) recipient (Target Group A)
- Qualified Veterans (Target Group B)
- Qualified Ex-Felons (Target Group C)
- Qualified Designated Community Resident (Target Group D)
- Vocational Rehabilitation Referrals (Target Group E)
- Qualified Summer Youth (Target Group F)
- Qualified Supplemental Nutrition Assistance Program (SNAP) Recipients (Target Group G)

- Qualified Supplemental Security Income Recipient (Target Group H)
- Qualified Long Term TANF Recipients (Target Group I)
- Qualified Long Term Unemployment Recipients (Target Group L)

V. EDD RESPONSIBILITIES

It is agreed that EDD will:

- A. Ensure that information retrieved from SAWS database, its agents (county welfare departments), or its agents' contractors, will be confidential and used solely for determining WOTC eligibility. EDD will take all necessary steps to accomplish this, including, but not limited to, complying with California Welfare and Institutions Code section 10850.
- B. EDD shall ensure that it complies with all policies and procedures for accessing data via the SAWS database. This includes all EDD personnel accessing SAWS data will review and sign the SAWS "User Security and Acceptable Use Policy (Exhibit A), acknowledging their understanding of proper system use, prior to being granted access.
- C. Entity shall maintain records of signed acknowledgments and make them available for audit upon request by SAWS.
- D. Promptly notify SAWS in case of any suspected data breach or unauthorized access.
- E. EDD will use the data elements below to conduct WOTC-related eligibility searches within the SAWS database:
 - Full Name (First and Last Name)
 - Date of Birth
 - Address
 - Social Security Number
 - Dates and Timeframes of Benefits Received

VI. CalSAWS RESPONSIBILITIES

It is agreed that SAWS will, through its employees, agents, or agents' contractors:

- A. Provide credentials and access to authorized EDD employees to SAWS data and recipient benefit information via Amazon Web Service's (AWS) platform and front-end user access.
- B. Ensure the accuracy and availability of the WOTC data specifically for WOTC Target Groups A, G, H, and I.
- C. Notify EDD of any planned system changes, maintenance, or outages that may affect data availability.

VII. GENERAL PROVISIONS

A. LAWS AND REGULATIONS

1. This MOU is entered into and subject to applicable Federal and State laws, regulations, and directives.
2. The conduct of the parties to this MOU shall be in accordance with Title VI of the Civil Rights Act of 1964, and the rules and regulations promulgated thereunder.
3. EDD and SAWS agrees to comply with the Americans with Disabilities Act (ADA) of 1990, which prohibits discrimination on regulations, guidelines, and interpretations issued thereto.

B. MODIFICATION AND TERMINATION

1. This MOU may be amended at any time by written consent of both parties.
2. Either party may terminate this MOU upon thirty (30) days written notice given to the other party.
3. This MOU is not valid until signed by both parties.

VIII. DATA and SYSTEM SECURITY

EDD agrees to maintain technical and procedural system security safeguards – which at a minimum will be consistent with the California Department of Technology Statewide Information Management Manual (SIMM 5300), to protect SAWS data from unauthorized physical and electronic access. Methods applied are subject to annual review and approval by SAWS, upon written request to EDD.

CalSAWS reserves the right to disable and/or terminate accounts, including those used for API connectivity or access, in the event that system activity warrants it. In such cases, EDD will be notified immediately and provided with a summary of the discovery that led to the action, allowing EDD to take necessary courses of action (i.e. internal investigation).

IX. PROJECT CONTACTS

The contact person on behalf of SAWS is:

Holly Murphy
11971 Foundation Place, Gold River, CA 95670
(916) 282-3806
MurphyH@calsaws.org

The contact person on behalf of EDD is:

Leslie Glover
2901 50th Street, Sacramento, CA 95817
(916) 227-1393
Leslie.Glover@edd.ca.gov

Either party may make changes to the information above by giving written notice to the other party. Said changes shall not require an amendment to this Agreement.

IV. SIGNATURES

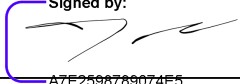
State of California
Employment Development Department

California Statewide
Automated Welfare System

By: Shelly Tarver

**Shelly Tarver, Division Chief
Northern Workforce Services**

Date: 5-22-2025

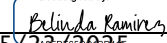
Signed by:
By: 
ATE2598789074E5...

**Julie Erdkamp, Executive Director
CalSAWS**

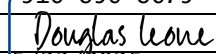
Date: 5/23/2025

READ and ACKNOWLEDGED: Information Security Officer (or authorized official responsible for business' information security program)

California Statewide Automated Welfare System (CalSAWS)

Name (Printed):	Belinda Ramirez
Title:	Chief Information Security Office
Email Address:	RamirezB@calsaws.org
Phone:	916-282-3653
Signature:	
Date Signed:	5/23/2025

Employment Development Department (EDD)

Name (Printed):	Douglas Leone
Title:	Division Chief, Cyber Security Division
Email Address:	Douglas.Leone@edd.ca.gov
Phone:	916-839-8879
Signature:	
Date Signed:	5/23/2025



User Security and Acceptable Use Policy

08/26/2024

User Security and Acceptable Use Policy

CalSAWS	DOCUMENT APPROVAL HISTORY	
	Work Product Owner	CalSAWS Consortium
	Prepared By	CalSAWS Consortium
	Reviewed By	CalSAWS Consortium
	Approved By	Consortium CISO/ISO

DATE	DOCUMENT VERSION	REVISION DESCRIPTION	AUTHOR
03/23/2021	1.0	Final	CalSAWS Consortium
07/21/2022	1.1	Update review table	CalSAWS Consortium
07/31/2023	1.2	Update Purpose and Scope sections. Review of Related Policies links, formatting, and added TOC	CalSAWS Consortium
04/30/2024	2.0	Added: 1. Review and Update, 2. Strictly Prohibited headers; Merged: 1. Acceptable Use Requirements into General Provisions, 2. Email & Other Forms of Communication into Email Responsibilities, 3. Other Security Responsibilities into System Operations and Physical Security; Formatting; Globally Replaced "should" with "must"; Updated: Roseville Conference Room in Physical Security; Updated Reference Table and links; Added clarification to Protected Data; 4. Removed reference to CalSAWS Information Security Policy	CalSAWS Consortium



User Security and Acceptable Use Policy

08/01/2024	3.0	Update 3.2 – Remove Sensitive information; 3.2.1 “Responsibilities” is now 3.2 “Data Protection”; Update 3.3 re- CalSAWS email usage; Remove Strictly Prohibited subsection headers; Update non CalSAWS email use statements; Remove Personal Information Section (refer to Data Classification Policy instead)	CalSAWS Consortium
08/12/2024	3.1	Update descriptions to revision table for 3.0; Update Reference Table (removing references that were removed with PI Section); Correct typos	CalSAWS Consortium
08/26/2024	3.2	Correct typo in 3.6	CalSAWS Consortium

APPROVAL DATE	APPROVED VERSION	REVIEWED AND APPROVED BY
07/15/2021	1.0	Consortium CISO
07/22/2022	1.1	Consortium CISO
08/03/2023	1.2	Consortium CISO
05/01/2024	2.0	Consortium CISO
08/02/2024	3.0	Consortium ISO
08/12/2024	3.1	Consortium ISO
08/26/2024	3.2	Consortium ISO

How to contact us

If you have questions about this policy, please contact CalSAWS Consortium Security at: Consortium.SecPolicy@calsaws.org



User Security and Acceptable Use Policy

Table of Contents

1. POLICY OVERVIEW 5

1.1. PURPOSE 5

1.2. SCOPE 5

1.3. REVIEW AND UPDATE 5

1.4. COMPLIANCE 5

2. POLICY REQUIREMENTS 5

2.1. GENERAL PROVISIONS 5

3. SECURITY REQUIREMENTS 6

3.1. PASSWORD RESPONSIBILITIES 6

3.2. DATA PROTECTION 6

3.2.1. Protected Data 7

3.2.2. Personally Identifiable Information (PII) 7

3.2.3. Sensitive Information 8

3.3. EMAIL AND OTHER FORMS OF COMMUNICATION 9

3.4. RESPONSIBILITIES FOR CHAT APPLICATIONS AND SERVICES 10

3.5. PRIVACY AND MONITORING 10

3.6. INCIDENT HANDLING 11

3.7. PHYSICAL SECURITY RESPONSIBILITIES 11

3.8. PERSONAL RIGHTS, HARASSMENT, AND WORKPLACE HOSTILITY 12

3.9. INFRINGEMENT 13

3.10. UNAUTHORIZED ACCESS 13

3.11. SYSTEM OPERATIONS 13

3.12. UNETHICAL BEHAVIOR 14

3.13. HARDWARE AND SOFTWARE ACCEPTABLE USE 14

3.14. PRODUCTION DATA 14

3.15. LAPTOPS AND PORTABLE DATA STORAGE DEVICES 15

4. RELATED POLICIES 15

5. REFERENCES 16



User Security and Acceptable Use Policy

1. POLICY OVERVIEW

1.1. PURPOSE

The purpose of this document is to define the principles and guidelines that are designed to provide CalSAWS with a formalized, documented User Security and Acceptable Use Policy that must be followed to ensure compliance with Confidentiality, Integrity, and Availability (CIA) of CalSAWS information systems.

1.2. SCOPE

This policy applies to all systems within the CalSAWS organization, including systems operated by the CalSAWS Consortium, vendors, contractors, sub-contractors, or third-party providers, systems owners, operators, and personnel, referred to as CalSAWS systems owners and operators.

1.3. REVIEW AND UPDATE

The Consortium Security Team reviews this document, and all associated CalSAWS artifacts annually using the ¹*Consortium Security Document Review Procedure*.

1.4. COMPLIANCE

All CalSAWS processes and procedures must implement the policy outlined in this document, in compliance with ²*NIST 800-53 Rev 4*, documented CalSAWS standards, as well as applicable local, state, and federal laws.

In the event this policy conflicts with another CalSAWS policy or a contractual requirement, the more restrictive policy or requirement will take precedence.

Every Consortium employee, Contractor employee and subcontractor that rolls onto the CalSAWS engagement is required to review and formally acknowledge this policy within 30 days of rolling onto the project and annually thereafter.

2. POLICY REQUIREMENTS

2.1. GENERAL PROVISIONS

CalSAWS systems, including but not limited to computer equipment, software, operating systems, storage media, network access/accounts providing electronic mail, web browsing, FTP, and any data that is the property of CalSAWS must be used in a secure manner, and may only be used for authorized CalSAWS business purposes relating to the CalSAWS Project.



User Security and Acceptable Use Policy

Under no circumstances may personnel engage in any activity that is illegal under local, state, or federal law while utilizing CalSAWS assets and information.

Personnel must not take any actions that could cause harm to CalSAWS systems, resources, assets, facilities, or personnel.

3. SECURITY REQUIREMENTS

3.1. PASSWORD RESPONSIBILITIES

Personnel are responsible for maintaining the secrecy of their passwords and are responsible for any misuse of their accounts as a result of inappropriately disclosed passwords.

1. Passwords to CalSAWS systems must be created, protected, and maintained in conformance with this policy.
2. Personnel are responsible for upholding password policies, even if the system does not or cannot require that all requirements be met.
3. Passwords must be entered each time they are requested and may not be stored on the local machine.
4. The use of approved password management software is allowed and may increase the likelihood of using stronger passwords.
5. In the event that personnel are locked out of an account, said personnel must contact Help Desk for assistance in resetting password.

Regarding Passwords, the following is strictly prohibited:

1. The disclosure of personnel passwords
2. Requesting the password of other personnel
3. The saving of passwords by use of "save password to this machine" or "remember my password on this computer"
4. Using any unauthorized third-party application to access or tamper with passwords

3.2. DATA PROTECTION

1. Personnel must safeguard Protected Data about security designs or implementations to prevent access by unauthorized persons.
2. Protected Data that is in electronic format must be protected by enabling password protection, stringent file permissions, or using an approved encryption mechanism. For details on acceptable encryption, please contact CalSAWS Technical Support.
3. Protected Data that is in printed format must be placed in a locked drawer or locked cabinet when not in use.

User Security and Acceptable Use Policy

4. When printing Protected Data, documents must be immediately removed from the printer.
5. Prior to leaving work area, personnel must log off from, or electronically lock their computers (including PCs, laptops, servers, and workstations).
6. All computers connected to the CalSAWS network under personnel control and use must be configured to automatically enable a password-protected screensaver or lock screen after no more than 10 minutes of inactivity.
7. Special care must be exercised when removing Protected Data from the facility. Personnel must ensure that such information is protected in a comparable or superior manner to how it is protected in a CalSAWS facility.
8. Portable devices such as smart phones with access to Protected Data must be configured to require password authentication prior to granting access.
9. Data on smart phones and other portable devices must be encrypted in transit and at rest.
10. Protected Data must be labeled as such, whether in electronic or printed form.

Regarding Protected Data, the following is prohibited:

1. Personnel must not provide non-public CalSAWS project-related information, such as names of personnel, contact information, user IDs, or project details ("Protected Data") to any unauthorized destinations or persons, without first confirming with their supervisor to whether the release of such Protected Data is acceptable.
2. Protected Data may not be removed from a CalSAWS facility unless approved by CalSAWS Project Management.

Refer to the *CalSAWS Data Classification Policy* for comprehensive details on classifying and protecting information.

3.2.1. PROTECTED DATA

Protected data is data that would have an adverse impact if publicly disclosed. Protecting the confidentiality and integrity of protected data is required. Only authenticated users with a need to know may access or modify sensitive data. This is the minimum data classification for all non-public data.

Examples: Network firewall configurations, known security vulnerabilities.

3.2.2. PERSONALLY IDENTIFIABLE INFORMATION (PII)

Personally Identifiable Information (PII) is a special subset of Protected Data. DHS defines PII as any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, visitor to the U.S., or employee or contractor.



User Security and Acceptable Use Policy

Examples: Name, address, phone number, email address.

3.2.3. SENSITIVE INFORMATION

Sensitive PII is Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII requires stricter handling guidelines because of the increased risk to an individual if the data are compromised.

Some categories of PII are “sensitive” as stand-alone elements. Examples include SSN, driver’s license or state identification number, passport number, Alien Registration Number, or financial account number.

Other data elements include citizenship or immigration status, medical information, ethnic, religious, sexual orientation, or lifestyle information, and account passwords, in conjunction with the identity of an individual (directly or indirectly inferred).

Sensitive PII (if stand-alone)

- Social Security number
- Driver’s license or state ID number
- Passport number
- Alien Registration number
- Financial account number
- Biometric identifiers

If paired with another identifier

- Citizenship or immigration status
- Medical information
- Ethnic or religious affiliation
- Sexual orientation
- Account passwords
- Last 4 digits of SSN
- Date of birth
- Criminal history
- Mother’s maiden name

3.3. EMAIL AND OTHER FORMS OF COMMUNICATION

Personnel must utilize their CalSAWS email accounts to conduct CalSAWS-related business. The Consortium manages and administers the CalSAWS.org email accounts to conduct project business. The use of non-CalSAWS email address/domains is prohibited. This includes the use of subcontractor email domains and/or personal email domains. CalSAWS email addresses must be utilized for all CalSAWS business purposes. Additionally, personnel must:

1. Be aware that written communications may be subject to public disclosure pursuant to federal and state law, specifically the ³*Freedom of Information Act (FOIA)* and the ⁴*California Public Records Act (CPRA)*.
2. Immediately open and act on any security message sent by CalSAWS Technical Support. Failure to do so can result in system compromise or data disclosure.
3. Use caution when determining whether to open emails or click links received from:
 - Unknown senders, as they may contain - or link to sites containing - viruses, worms, or Trojan horse code.
 - Known individuals if the email subject or contents seem out of character for that individual. In such a case, personnel must contact the sender and verify the validity of the email before opening it whenever possible.

In the event personnel receives a suspicious email, personnel must:

1. Notify technical support of suspected spam or phishing emails.
2. Always let CalSAWS Technical Support handle communication to the project, remediation, and prevention.
3. Never take any action regarding virus notifications, except to notify CalSAWS Technical Support (unless it is received from CalSAWS Technical Support).

The following activities, as they relate to use of email and other forms of communication, are prohibited:

1. Sending unsolicited email messages, including the sending of chain letters, "junk mail," or other advertising material or mass mailings to individuals who did not specifically request such material (email spam).
2. Sending or arranging to receive information that violates state or federal laws.
3. Sending any material that may defame, libel, abuse, embarrass, tarnish, present a bad image of, or portray in false light, CalSAWS, the organizations in CalSAWS, the recipient, the sender, or any other person.
4. Sending pornographic, racist, or other material that is generally considered offensive.

User Security and Acceptable Use Policy

5. Sending malicious code.
6. Forging email header information.
7. Soliciting email for any other email address (e.g., registering another user to receive junk mail).
8. Sending anonymous emails.
9. Distributing or posting non-public CalSAWS information (e.g., Protected Data) of any kind outside of CalSAWS, without proper authorization by a CalSAWS manager.

3.4. RESPONSIBILITIES FOR CHAT APPLICATIONS AND SERVICES

Chat applications and services typically do not provide end-to-end encryption services. Without end-to-end encryption, chat conversations are vulnerable to interception by unauthorized third parties. Personnel must never discuss Protected Data or transmit files containing Protected Data over chat services.

Chat services can be susceptible to viruses, as they provide an unprotected gateway from the Internet into the CalSAWS network. Files must not be transferred via chat applications. If there is no other alternative, such as SFTP or email, approval must be obtained from the CalSAWS Consortium Security Office. Any files received via chat file transfer must be scanned with a virus scanner prior to being opened or executed.

As with email, personnel must never click on a URL link sent via chat if it appears unfamiliar or out of character for the sender. Personnel must contact the sender regarding any link that appears suspicious and ask about the validity of the link before attempting to access the site.

3.5. PRIVACY AND MONITORING

The workstations, laptops, and user accounts assigned to personnel are provided to enable them to perform their jobs in the most efficient and effective way possible. However, personnel are not entitled to any expectation of privacy in the materials or information that is created, sent, or received by them on CalSAWS systems. To the extent permitted by local, state, and federal laws, the CalSAWS contracts, authorized personnel (such as the CalSAWS Systems Security Officer, members of the security team, CalSAWS technical support, CalSAWS project staff, CalSAWS authorized representatives, etc.) may examine any materials and information stored on CalSAWS systems without prior notice, as they feel appropriate. Some examples of situations may include investigation for a suspected breach of security, for the prevention or detection of crime, and other legally permissible situations.

Subject to local, state, and federal laws, the CalSAWS contracts, CalSAWS may monitor any and all aspects of its computerized resources used by personnel, including, but not limited to, monitoring sites visited by users on the Internet, monitoring chat groups and newsgroups, reviewing material downloaded from or uploaded to the Internet by personnel, and reviewing



User Security and Acceptable Use Policy

email sent and received by personnel. Wherever possible, monitoring must be carried out by methods which prevent misuse, such as automated monitoring software. Personnel must understand that CalSAWS may use automated monitoring software to monitor material created, stored, sent, or received on the CalSAWS network to ensure that inappropriate material is not created on, or transmitted via CalSAWS systems, and that inappropriate use of CalSAWS systems does not occur.

3.6. INCIDENT HANDLING

Personnel must promptly report any suspicion of, or occurrence of, unauthorized activities as outlined in the organization's incident response process. This includes suspected password compromise and inappropriate data disclosure. In the case of virus infection, or phishing suspicion, personnel must immediately contact CalSAWS Technical Support. Personnel must not take any action on their computers as such actions could adversely affect a security investigation or the ability to safely eradicate malicious code.

3.7. PHYSICAL SECURITY RESPONSIBILITIES

Personnel must immediately notify their supervisor if they feel that complying with this policy would put them in such danger.

1. Personnel must physically lock down their laptops when left unattended with an approved cable lock device or in a locked drawer or locked cabinet.
2. Personnel must safeguard any mobile devices and removable storage media containing CalSAWS information by concealing them in locked drawers or locked cabinets when left unattended.

Regarding physical access to the Project Management Office (PMO) or the CalSAWS project sites personnel must adhere the following:

1. All CalSAWS project staff must visibly wear their project ID badge each day while on site. If any CalSAWS project staff has lost their badge, they must notify the Project Management Office (PMO) immediately so the lost badge can be deactivated, and a new one can be issued.
2. All visitors (anyone who is not staffed on the project and does not have a CalSAWS project ID badge) must sign in at the front desk upon entry and sign out before exiting the CalSAWS facility.
3. Visitors must be provided with a CalSAWS visitor badge that they must visibly wear while onsite; this badge is an inactive badge that must not open doors that have a proximity access pad. If necessary, a temporary proximity access badge can be checked out from PMO. Otherwise, these visitors must be escorted by the CalSAWS staff with whom they are meeting.



User Security and Acceptable Use Policy

4. All visitors must sign out at the front desk and return any CalSAWS visitor badges and temporary proximity access badges before leaving the site.
5. Any suspicious persons noticed during non-business hours must be reported to the on-site security guard.

For onsite workgroups or other large onsite meetings:

1. The meeting coordinator must obtain a list of attendees from the county (or other appropriate organization) and provide that list to the CalSAWS receptionist in advance of the meeting to help expedite the sign-in process.
2. A temporary proximity access badge that allows access to locked doors with a proximity access pad can be issued to the meeting/ workgroup coordinator and shared among the visitors.
3. Large onsite meetings at the project site must be scheduled in *Cypress Conference Room* (for the Roseville Facility) when possible so that visitors can leave and re-enter the site without a proximity access badge.

Regarding physical security, the following is prohibited:

1. Personnel must not tamper with or circumvent installed physical facility security measures.
2. When the facility doors are locked, personnel must not allow anyone access to the facilities unless the individual can be positively identified as authorized to access the facilities after hours.
3. Personnel must not put themselves in physical danger to obey this policy (e.g., protecting the facility's physical security does not include wrestling a gun from an intruder).

3.8. PERSONAL RIGHTS, HARASSMENT, AND WORKPLACE HOSTILITY

The following activities are strictly prohibited:

1. Violating the rights of any person or company.
2. Using CalSAWS assets to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws.
3. Harassing anyone via email, telephone, paging, or any other means of communication, whether through language, frequency, or size of messages.
4. Browsing websites containing, storing, or displaying information or materials that are explicit, pornographic, or hate-based.

3.9. INFRINGEMENT

Infringement of the intellectual property rights of others is a serious offense that could result in the prosecution of not only the individual perpetrator, but also of CalSAWS if the offense was carried out using CalSAWS assets and information.

Regarding infringement, the following is prohibited:

1. Violating information protected by copyright, trade secret, patent, trademark, or other intellectual property rights, or similar laws or regulations, including, but not limited to, the installation, storage, or distribution of "pirated" or other software products that are not appropriately licensed for use by CalSAWS.
2. By definition, anything posted on the Internet that is an original work (including email, pictures, jokes, artwork, music, etc.) is protected by copyright law(s), whether or not it is explicitly indicated that the work is copyrighted, or the copyright (©) symbol is included. Therefore, personnel may not use such original works of authorship (e.g., by using "cut and paste" or "copy and paste") or download music or videos without the author's (or artist's) express permission. In a text-based document, merely changing a few words or "scrubbing" (i.e., removing) the specific references to names or other identifiers in the document is not enough to avoid copyright infringement issues and therefore is not acceptable.

3.10. UNAUTHORIZED ACCESS

The following are considered forms of unauthorized access, and as such are prohibited:

1. Stealing electronic files or copying them without permission.
2. Browsing the private files or accounts of others.
3. Attempting to access data or resources to which the individual has not been granted explicit permissions.

3.11. SYSTEM OPERATIONS

Personnel must maintain virus scanning utilities, personal firewalls, or other programs designed to protect systems, users, or information in good working order, with approved configurations intact.

With regards to system operations, the following is prohibited:

1. Introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
2. Conducting unauthorized port or vulnerability scans or executing any form of unauthorized network monitoring.

User Security and Acceptable Use Policy

3. Tampering with or circumventing user authentication or security of any host, network, or account.
4. Interfering with or denying service to any user or system/resource.
5. Using any program/script/command, or sending messages of any kind, with the intent to interfere with or disable a user's session.
6. Disabling or modifying any legal notice or warning banners on CalSAWS systems.
7. Personnel must not set up or assist in the configuration of unauthorized network or telephone access points (e.g., modems or wireless access points).
8. Performing unauthorized activities that may degrade the performance of systems, such as:
 - Playing electronic games
 - Downloading large files, streaming music, or video from the internet
 - Storing or downloading music, videos, and/or pictures on your computer

3.12. UNETHICAL BEHAVIOR

The following activities are considered unethical, and are therefore prohibited at CalSAWS:

1. Promoting or maintaining a personal or private business, or otherwise using CalSAWS assets or information for personal gain.
2. Engaging in financial transactions such as online gambling, using CalSAWS assets or information.

3.13. HARDWARE AND SOFTWARE ACCEPTABLE USE

Personnel must only use hardware and software that is supplied by the project or is otherwise authorized by their supervisor or CalSAWS technical support. Supervisors that do not know if hardware/software must be authorized must consult CalSAWS technical support or the CalSAWS Security Officer.

Installing or executing programs on CalSAWS systems or hardware without authorization, including but not limited to, those from CDs/DVDs, audio/video streaming software or files, file shares, floppies, or downloaded from the internet, is prohibited.

3.14. PRODUCTION DATA

1. CalSAWS production data (in any format) must not leave the project site unless properly secured and then only for the purpose of transfer to a location authorized by the CalSAWS project manager.
2. CalSAWS production data must be transported electronically ONLY by secure FTP, CalSAWS SharePoint or by encrypted email. You MAY NOT USE unencrypted email or Instant Messenger applications to transfer data.



User Security and Acceptable Use Policy

- 3. All printed production data/material must be shredded or stored in a locked cabinet on the premises at all times.
- 4. Making electronic copies of production data for the purposes for unauthorized usage is prohibited.
- 5. Transmission of production data by fax is prohibited.

3.15. LAPTOPS AND PORTABLE DATA STORAGE DEVICES

Client Protected Data is only allowed on CalSAWS or encrypted portable storage devices such as memory sticks and external USB drives or such devices as CalSAWS permits outside vendors and contractors to utilize in the performance of CalSAWS-related work.

4. RELATED POLICIES

POLICY	LOCATION
Data Classification Policy	CalSAWS SharePoint: CalSAWS Data Classification Policy

5. REFERENCES

NO.	REFERENCE
1	Consortium Security Document Review Procedure
2	Joint Task Force Transformation Initiative Interagency Working Group (2013) Security and Privacy Controls for Federal Information Systems and Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-53, Rev. 4, Includes updates as of January 22, 2015. https://doi.org/10.6028/NIST.SP.800-53r4
3	Freedom of Information Act (FOIA)
4	California Public Records Act (CPRA)