

CalSAWS User Security and Acceptable Use Policy

Overview

CalSAWS assets and information within the project's control and use must be used in a secure, approved, ethical, and lawful manner and in accordance with the terms and conditions of the CalSAWS contracts to appropriately protect such assets and information. This policy applies to all systems operated by the CalSAWS Joint Powers Authority (JPA) including the legacy C-IV, legacy CalWIN and LRS systems (hereafter collectively referred to as "CalSAWS Systems").

Purpose

The purpose of this Security and Acceptable Use Policy ("Policy") is to outline appropriate user security and acceptable use requirements relating to the CalSAWS assets and information that are within the project's control and use.

Scope

This Policy applies to all CalSAWS Project personnel across all organizations, as well as all outside vendors who are provided with access to CalSAWS Systems as part of the contract work such vendors are providing to CalSAWS (hereafter collectively referred to as "Personnel").

Compliance

Security and acceptable use, as described herein, are the responsibility of all Personnel. Non-compliance with the required measures and behaviors outlined in this Policy could pose significant business and legal risk to the CalSAWS Consortium, organizations in the Consortium, and/or the offending Personnel, and could negatively impact CalSAWS operations. Therefore, your full understanding and compliance with this Policy is mandatory. Failure to comply will be reported and appropriate action taken, which may include, but is not limited to, financial penalties, termination of employment, legal action, or other steps as appropriate. Applicable county discipline procedures will be followed for Consortium personnel. If you become aware of any breach or potential breach of this Policy by you, outsiders, or any Personnel, immediately contact your supervisor.

Precedence

Personnel must follow this Policy in addition to the acceptable use and security policies of their organization. In the event of a conflict between this Policy and their organization's policies, Personnel will adhere to the more stringent policy. Personnel will clarify policy conflict questions with their supervisor or CalSAWS Technical Support. Supervisors that do not know the right course of action must consult CalSAWS Security Officer.

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.

There is one general requirement with respect to use of CalSAWS systems:

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

Security Requirements

Password Responsibilities

The disclosure of Personnel passwords is strictly prohibited. Personnel are responsible for maintaining the secrecy of their passwords and will be responsible for any misuse of their accounts as a result of inappropriately disclosed passwords. No Personnel are authorized to request the password of other personnel, including Technical Support staff.

Passwords to CalSAWS systems must be created and maintained in conformance with this Policy and the CalSAWS Information Security Policy.

Personnel are responsible for upholding password policies, even if the system does not or cannot require that all requirements be met.

Sensitive Information

Personnel shall not provide non-public CalSAWS Project-related information, such as names of Personnel, contact information, user IDs, or project details ("Sensitive Information") to any unauthorized destinations, without first confirming with their supervisor whether the release of such Sensitive Information is acceptable. Sensitive Information 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.

Sensitive Information that is in printed format must be placed in a locked drawer or locked cabinet when not in use. When printing Sensitive Information, documents must be immediately removed from the printer.

Prior to leaving their work area, Personnel must log off from, or electronically lock their computers (including PCs, laptops, servers, and workstations). All computers connected to the CalSAWS network under Personnel control and use must be configured to automatically enable a password-protected screensaver after no more than 10 minutes of inactivity.

Special care must be exercised when removing Sensitive Information 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. Sensitive Information may not be removed from a CalSAWS facility unless approved by CalSAWS Project Management.

Any Personal Digital Assistant (PDA) device containing Sensitive Information must be configured to require password authentication prior to granting access. Where available, appropriate encryption mechanisms will be used.

Sensitive Information must be labeled as such, whether in electronic or printed form. Refer to the CalSAWS Data Classification Standard for additional details on classifying and protecting sensitive information.

Note: Sensitive Information should not be confused with confidential information. Confidential information consists of any oral, written or electronic information that either belongs to, has been developed by, or has been received from our client, CalSAWS, and has commercial value in their business, or the business of their affiliates, vendors, customers or clients and is not generally available to the public. Every Consortium employee, Contractor employee and subcontractor that rolls onto the CalSAWS engagement is required to review and formally acknowledge this policy.

Personal Information

Personnel shall comply with the provisions of Section 10850 and 18909 of the Welfare and Institutions Code, Division 19 of the California Department of Social Services Manual of Policies and Procedures, and all other statutory laws relating to privacy and confidentiality. The referenced Welfare and Institutions codes stipulate that the data is confidential and shall not be disclosed.

In order understand the definition of data, the California Civil Code applies. As defined in California Civil Code section 1798.82, "any person or business that conducts business in California, and that owns or licenses computerized data that includes **personal information**, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." (e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

- Social security number.
- Case Number
- Driver's license number or California Identification Card number.
- Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Personal Information may not be printed, faxed, emailed, or stored on a laptop. Personal Information may not be taken from the Application Development Facility. Exceptions to this must be authorized by Project Executive Management.

Email Responsibilities

Some Personnel may retain email accounts provided by their employer's (vendor or county). Such accounts are important for conducting confidential business and personnel matters. The Consortium manages and administers the CalSAWS.org email accounts to conduct project business.

Personnel shall utilize their CalSAWS email accounts to conduct CalSAWS-related business. Exceptions to the use of the CalSAWS email domain include the following:

- Non-Project communications
- Confidential personnel matters

Personnel must be aware that written communications may be subject to public disclosure pursuant to federal and state law, specifically the Freedom of Information Act (FOIA) and the California Public Records Act (CPRA). The CPRA was enacted in 1968 and codified as California Government Code § 6250 through § 6276.48. The fundamental precept of the CPRA is that government records shall be disclosed to the public, upon request, unless legally exempt from such disclosure or the public interest in nondisclosure clearly outweighs the public interest in disclosure. Some exemptions to public disclosure include:

- Preliminary drafts, notes, or memoranda that are not retained by the public agency in the ordinary course of business
- Personnel, medical records, or similar files, the disclosure of which would constitute an unwarranted invasion of personal privacy
- Applications or records concerning any individual in connection with any form of public social services under the California Welfare & Institutions Code §10850
- Deliberative processes, discussions, or negotiations
- Trade secrets or proprietary information
- Attorney-client privileged communications
- Records pertaining to pending litigation to which the agency is a party, or to claims, until the litigation or claim has been finally adjudicated or otherwise settled

Personnel must use caution when opening email attachments received from unknown senders, as they may contain viruses, worms, or Trojan horse code. Personnel should also be cautious of email from known individuals if the email subject or contents seem out of character for that individual. In such a case, Personnel should contact the sender and verify the validity of the email before opening it whenever possible.

Personnel must never reply to spam or take actions as requested in the message, such as clicking on a link, doing what it says about a virus, replying, or asking to be removed

from the mailing list. "Unsubscribing" from unsolicited spam messages typically serves to alert the sender that a valid email address exists and will generally result in even more spam being sent. Spam messages should be disregarded and promptly deleted. Personnel should also notify technical support if the spam becomes a nuisance. Personnel must 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.

Unless it is received from CalSAWS Technical Support, Personnel must never take any action regarding virus notifications. Furthermore, Personnel must always let CalSAWS Technical Support handle communication to the project, remediation, and prevention. Personnel are advised that many publicly distributed emails containing virus warnings are hoaxes and following such emails can result in computer damage.

Instant Messenger Responsibilities

Instant messaging services typically do not provide encryption services and are thus not secure. Without encryption, instant messenger conversations are vulnerable to interception by unauthorized third parties. Personnel must never discuss Sensitive Information or transmit files containing Sensitive Information over unencrypted instant messaging services.

Instant messaging services make the CalSAWS network susceptible to viruses, as they provide an unprotected gateway from the Internet into the CalSAWS network.

Personnel should only use instant messaging file transfer as a last resort, if email is unavailable. Any files received via instant messenger file transfer must be scanned with a virus scanner prior to being opened or executed.

A common mechanism for propagating instant messenger viruses is via URL links. Personnel should never click on a URL link sent via instant messenger if it appears unfamiliar or out of character for the sender. Personnel should contact the sender of any link that appears suspicious and ask about the validity of the link before attempting to access the site.

Other Security Responsibilities

Personnel are responsible for the following to help maintain CalSAWS system security:

- Personnel are prohibited from conducting unauthorized port or vulnerability scans or executing any form of unauthorized network monitoring.
- Personnel must not tamper with or circumvent user authentication or security of any host, network, or account.
- 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.
- Personnel may not disable or modify any legal notice or warning banners on CalSAWS systems.
- Personnel may not tamper with or circumvent installed physical facility security measures.
- Personnel must safeguard Sensitive Information about security designs or implementations to prevent access by unauthorized persons.

- Personnel must not set up or assist in the configuration of unauthorized network or telephone access points (e.g., modems or wireless access points).

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 email sent and received by Personnel. Wherever possible, monitoring will 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.

Incident Handling

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

Physical Security

During the day, Personnel must physically lock down their laptops with an approved cable lock device.

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.

With regard to physical access to the Project Management Office (PMO) or the CalSAWS project sites (Norwalk, Rancho Cordova and Roseville, Ca), Personnel must adhere the following:

- 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.
- 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.
 - Visitors will be provided with a CalSAWS Visitor badge that they should visibly wear while onsite; this badge will be an inactive badge that will 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 should be escorted by the CalSAWS staff with whom they are meeting.
 - For onsite workgroups or other large onsite meetings:
 - The meeting coordinator should 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.
 - 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. Large onsite meetings at the project site should be scheduled in Sutter Conference Room in Suite 150 when possible so that visitors can leave and re-enter the site without a proximity access badge.
 - All visitors must sign out at the front desk and return any CalSAWS Visitor badges and temporary proximity access badges before leaving the site.
- 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. Personnel should 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), however, they should immediately notify their supervisor if they feel that complying with this Policy would put them in such danger. Any suspicious persons noticed during non-business hours should be reported to the on-site security guard.

Acceptable Use Requirements

CalSAWS assets and information are to be used for authorized business purposes relating to the CalSAWS Project only.

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

Personal Rights, Harassment, and Workplace Hostility

The following activities are strictly prohibited:

- Violating the rights of any person or company.

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

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. As such, the following are strictly prohibited:

- 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.
- 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.

Unauthorized Access

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

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

System Operations

The following are prohibited as they interfere with normal systems operations:

- Introducing malicious programs into the network or server (e.g., viruses, worms, Trojan horses, email bombs, etc.).
- Interfering with or denying service to any user or system/resource.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's session.
- 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

Unethical Behavior

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

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

Email and Other Forms of Communication

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

- 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).
- Sending or arranging to receive information that violates state or federal laws.
- 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.
- Sending pornographic, racist, or other material that is generally considered offensive.
- Sending malicious code.
- Forging email header information.
- Soliciting email for any other email address (e.g., registering another user to receive junk mail).
- Sending anonymous emails.
- Distributing or posting non-public CalSAWS information (e.g., Sensitive Information) of any kind outside of CalSAWS, without proper authorization by a CalSAWS manager.

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 should 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.

Security Requirements for Project Staff

- CalSAWS Production Data (in any format) may 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
- CalSAWS Production Data may 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.
- All printed Production data/material must be shredded or stored in a locked cabinet on the premises at all times.
- Making electronic copies of production data for the purposes for unauthorized usage is prohibited
- Transmission of production data by fax is prohibited

Laptops and Portable Data Storage Devices

Personal and Sensitive Information must be encrypted and/or password protected on any laptop, CalSAWS or otherwise. Client Sensitive Information 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.

Contact

Questions related to this Policy can be addressed to CalSAWS Technical Support by calling or emailing Tech.Support@CalSAWS.org, or CalSAWS Information and Privacy Security Office at Consortium.Tech.Security@CalSAWS.org.

1.2 Referenced Documents

A. CalSAWS Information Security Policy
--

I HAVE READ THIS AGREEMENT AND HAVE TAKEN DUE TIME TO CONSIDER IT PRIOR TO SIGNING. I UNDERSTAND THIS ENTIRE CALIFORNIA STATEWIDE AUTOMATED WELFARE SYSTEM USER SECURITY AND ACCEPTABLE USE POLICY AND AGREE TO ABIDE BY ALL OF ITS PROVISIONS:

[SIGNATURE BLOCKS TO BE ADDED]