



Countywide Information Security Policies

ABSTRACT

Countywide Information Security Policies address the highest-level policy of the County and include all departments whether lead by appointed or elected officials. These policies are meant to ensure that the County conducts itself in a meaningful, standard manner as a model of protecting County owned or controlled informational assets. These policies are reviewed on an annual basis by the County Information Security Committee to see if they are successfully supporting Countywide Information Security Program requirements. Additional departmental policy may be needed to address specific business requirements.

Table of Contents

RESPONSIBILITIES OVERVIEW	3
ACCESS CONTROL POLICY	4
PERSONALLY OWNED DEVICE POLICY	11
WORKSTATION USE AND SECURITY POLICY	14
IDENTIFICATION AND AUTHENTICATION POLICY	16
AUDITING AND ACCOUNTABILITY POLICY	21
CONFIGURATION MANAGEMENT POLICY	24
ASSET MANAGEMENT POLICY	27
PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY	32
FACILITY ACCESS CONTROL POLICY	39
MAINTENANCE POLICY	42
MEDIA PROTECTION POLICY	45
SECURITY AWARENESS AND TRAINING POLICY	49
PERSONNEL SECURITY POLICY	52
RISK MANAGEMENT POLICY	56
RISK ASSESSMENT POLICY	59
VENDOR AND THIRD-PARTY MANAGEMENT	62
BUSINESS ASSOCIATE AGREEMENTS	65
INFORMATION SYSTEM AND SERVICES ACQUISITION POLICY	67
CUSTOM DEVELOPED SOFTWARE POLICY	73
GENERATIVE ARTIFICIAL INTELLIGENCE (AI) USE POLICY	81
INFORMATION SYSTEM AND COMMUNICATIONS PROTECTION POLICY	89
INFORMATION SYSTEM INTEGRITY POLICY	94
INCIDENT RESPONSE POLICY	99
CYBERCRIME AND RANSOMWARE INCIDENT RESPONSE POLICY	102
CONTINGENCY PLANNING POLICY	105
DATA CLASSIFICATION POLICY	110
SECURITY MANAGEMENT POLICY	113
INTERNET OF THINGS (IOT) AND OPERATIONAL TECHNOLOGY (OT) DEVICES POLICY	116
CLOUD SERVICES SECURITY POLICY	120
ENCRYPTION KEY AND CERTIFICATE MANAGEMENT POLICY	124
ZERO TRUST ARCHITECTURE POLICY	129
APPENDIX A: GLOSSARY	132
COMMON TERMS AND DEFINITIONS	132
APPENDIX B: ACRONYMS	159
COMMON ABBREVIATIONS	159
APPENDIX C: DEPARTMENT LISTING	161

APPENDIX D: DEVICE TYPE LISTING 163
APPENDIX E: SECURITY AND PRIVACY CONTROL CATALOG COMPLIANCE MAPPING 164

RESPONSIBILITIES OVERVIEW

Departmental Responsibilities

- Departments must read, understand, and comply with all Countywide Information Security Policies.
- Departments are responsible for implementing and communicating these policies to all relevant users, staff, and management within their area of responsibility.
- Additional departmental policies and procedures may be developed to address specific business requirements.

Management Responsibilities

- County management assigns individual roles and responsibilities to ensure the accomplishment of Information Security Policy requirements.
- Management must ensure that policies are effectively enforced and that compliance is monitored.

Everyone’s Responsibility

- All individuals with access to County information resources must read, understand, and comply with the Information Security Policies.
- Certain policies apply universally and are the responsibility of every user, not just specific roles or departments

County IT Responsibilities

- County IT includes all information systems staff, departmental IT staff, and information systems business units across all County departments.
- The Information Systems Division (ISD) of the County Administrator’s Office provides centralized oversight.

Security Leadership

- The ISD Director designates a Chief Information Security Officer (CISO) to oversee and monitor cybersecurity programs Countywide.
- Department Directors must designate Department Information Security Officers (DISOs) to direct and implement cybersecurity programs within their departments.
- The CISO organizes a Countywide DISO program to coordinate activities and ensure policy alignment.

Policy #:	Title:	Effective Date:
SJC-SEC-POL-1	Access Control Policy	12/01/2023

PURPOSE

To ensure that County Information Technology (IT) access controls comply with County IT security policies, standards, and procedures.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. ACCESS AUTHORIZATION

County IT shall:

- a. Specify authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account.
- b. Authorize access to the information system based on a valid access authorization or intended system usage.
- c. For systems containing electronic protected health information (ePHI), implement specific procedures authorizing access to ePHI in accordance with the applicable requirements of the HIPAA Privacy Rule.
- d. Establish, document, review, and modify users' rights to access certain workstations, transactions, programs, or processes that are based on this and departmental authorization policies.

2. ACCOUNT MANAGEMENT

County IT shall (or other staff as applicable):

- a. Identify and select the following types of information system accounts to support organizational missions and business functions: individual, shared, group, system, guest/anonymous, emergency, contractor/vendor, temporary, and service.
- b. Establish conditions for group and role membership.
- c. Create, enable, modify, disable, and remove information system accounts in accordance with county standards and departmental procedures.

- d. Monitor the use of information system accounts. (See AUDITING AND ACCOUNTABILITY POLICY).
- e. Prohibit shared\group accounts from accessing confidential data (e.g., ePHI).
- f. Ensure that the information system automatically disables temporary and emergency accounts after usage. Configure contractor\vendor and temporary accounts with an automatic termination date no greater than 30 days from account creation, or as permitted by contract (e.g., Independent Contractor Agreement).
- g. Ensure that the information system automatically disables individual accounts after 90 days of inactivity unless authorized by the department head for longer leave/PTO etc., scenarios.

3. ACCESS ENFORCEMENT

County IT shall:

- a. Ensure that the information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies.
- b. Implement technical policies and procedures for electronic information systems that maintain confidential data (e.g., ePHI) to allow access only to those persons or software programs that have been granted access rights.
- c. For those departments or agencies covered by HIPAA (see HIPAA HYBRID ENTITY POLICY), implement policies and procedures to ensure that all members of the workforce have appropriate access to ePHI, as provided under 45 CFR 164.308(a)(4), and to prevent those workforce members who do not have access under that section from obtaining access to ePHI.
 - a. At a minimum, such departmental policies and procedures should identify workforce members by job classification who require access to ePHI, assign them unique IDs, assign those unique IDs to relevant security roles, and then grant access to ePHI based on security roles. Under no conditions should a workforce member gain access to ePHI using a generic or shared ID.

4. ACCESS CONTROL REVIEW

County IT shall:

- a. Periodically, but not less than annually, conduct an access control audit to review access of users to confidential data (e.g., ePHI).
- b. Periodically, but not less than annually, conduct a privileged access control audit to review access of users and accounts with privileged or administrative access to

information systems.

5. SEPARATION OF DUTIES

County IT shall:

- a. Separate duties of individuals as necessary, to prevent malevolent activity without collusion. Define application or system roles that segregate duties and assign individual accounts to those roles as authorized.

6. LEAST PRIVILEGE

County IT shall:

- a. Employ the principle of least privilege, allowing only authorized access for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
- b. Require that users of information system accounts, or roles, with access to separate privileged accounts, use non-privileged accounts or roles when accessing non-security functions.
- c. Restrict privileged accounts on the information system to least access required to perform the job.
- d. Ensure that the information system audits the execution of privileged functions.
- e. Ensure that the information system prevents non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards/countermeasures.

7. UNSUCCESSFUL LOGON ATTEMPTS

County IT shall ensure that the information system:

- a. Enforces a limit of consecutive invalid logon attempts by a user during a 20 minute window for five (5) unsuccessful attempts.
- b. Locks the account/node automatically for 10 minutes or until released by an administrator when the maximum number of unsuccessful attempts five (5) is exceeded.

8. SYSTEM USE NOTIFICATION

County IT shall ensure that the information system:

- a. Displays to users an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable state and federal laws, directives, policies, regulations, standards, and guidance and states informing that:

- i. Users are accessing a County information system.
- ii. Information system usage may be monitored, recorded, and subject to audit.
- iii. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties.
- iv. Use of the information system indicates consent to monitoring and recording.
- v. There are not rights to privacy.

9. SESSION LOCK

County IT shall ensure that the information system:

- a. Prevent further access to the system by initiating a session lock after 30 minutes of inactivity or upon receiving a request from a user.
- b. Retain the session lock until the user re-establishes access using established identification and authentication procedures.
- c. Conceal, via the session lock, information previously visible on the display with a publicly viewable image.

10. PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

County IT shall:

- a. Prohibit and deny access by shared, group or generic accounts to any confidential data (e.g., ePHI).

11. REMOTE ACCESS

County IT shall:

- a. Implement and maintain remote access services per the County Remote Access Standard.
- b. Ensure that the information system monitors and controls remote access methods.
- c. Ensure that the information system implements cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.
- d. Remote sessions shall be terminated after 15 minutes of inactivity requiring the user to authenticate again to access County resources
- e. All remote access infrastructures shall include the capability to monitor and record a detailed audit trail of each remote access attempt.

- f. Periodic assessments shall be performed to identify unauthorized remote connections. Results shall be used to address any vulnerabilities and prioritized according to criticality
- g. All remote access implementations that involve non-County infrastructures shall be reviewed and approved by both the department DISO and IT Information Security. This approval shall be received prior to the start of such implementation.

12. WIRELESS ACCESS

County IT shall:

- a. Implement and maintain wireless network services per the **County Wireless Networks Standard**.
- b. Restrict access to County wireless networks to authorized workforce members and devices.
- c. Establish separate guest wireless networks with no access to confidential data (e.g., ePHI) for use by the public, visitors, and vendors.
- d. Each department shall make a regular, routine effort to ensure that unauthorized wireless networks, access points, and/or modems are not installed or configured within its IT environments. Any unauthorized connections described above shall be disabled immediately.

13. ACCESS CONTROL FOR MOBILE DEVICES

County IT shall:

- a. Implement and maintain mobile device management systems and configurations per the **County Mobile Device Management Standard**.
- b. Authorize the connection of mobile devices managed by County mobile device management systems to County wireless networks and/or information systems.
- c. Prohibit and deny access by unmanaged mobile devices to County wireless networks and/or information systems except designated guest wireless networks.
- d. Employ full-device encryption or container encryption to protect the confidentiality and integrity of confidential information (e.g., ePHI) on approved mobile devices.

14. ACCESS MANAGEMENT FOR EPHI

For departments or agencies covered by HIPAA (see HIPAA HYBRID ENTITY POLICY), County IT shall:

- a. Implement specific policies and procedures authorizing and granting access to ePHI in accordance with the applicable requirements of the HIPAA Security Rule. Such departmental policies and procedures should identify workforce members by job classification who require access to ePHI, assign them unique IDs, assign those unique IDs to relevant security roles, and then grant access to ePHI based on security roles. Under no conditions should a workforce member gain access to ePHI using a generic or shared ID.
- b. Implement specific policies and procedures to regularly and periodically establish, document, review and modify workforce members' rights to access certain workstations, transactions, programs or processes that contain or process ePHI.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

DATE ISSUED/DATE REVIEWED

Date Issued:	04/15/2020
Date Reviewed:	03/11/2026

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Access Control (AC), NIST SP 800-12, NIST 800-46, NIST SP 800-48, NIST SP 800-77, NIST SP 800-94, NIST SP 800-97, NIST SP 800-100, NIST SP 800-113, NIST SP 800-114, NIST SP 800-121, NIST SP 800-124, NIST SP 800-164;

NIST Federal Information Processing Standards (FIPS) 199;
State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information
Management Manual (SIMM) et seq.
HIPAA Security Rule: Access Control: 45 CFR 164.312(a)(1)
HIPAA Security Rule: Automatic Logoff: 45 CFR 164.312(a)(2)(iii)
HIPAA Security Rule: Workforce Security: 45 CFR 164.308(a)(3)(i)

Policy #:	Title:	Effective Date:
SJC-SEC-POL-2	Personally Owned Device Policy	04/14/2025

PURPOSE

To establish users and County and/or IT expectations and requirements for using a personally owned device to access County data containing confidential data (e.g. electronic protected health information (ePHI)).

DEFINITIONS

Personally Owned Devices: Personal computing devices include, but are not limited to, removable media such as thumb or USB drives, external hard drives, laptop or desktop computers, smartphones or tablets owned by or purchased by employees, contract personnel, or other non-County users. The practice of utilizing personally owned devices is also known as BYOD (Bring Your Own Device)

Mobile Device: Any device used for electronic communication including, but not limited to electronic notebook, tablets, laptop computer, smart phones, iPad, iPhone, Android, palm computer, Treo, or any combination of handheld or mobile computer communication device.

Mobile Device Management (MDM): Software that secures, manages, and monitors mobile devices.

Data Loss Prevention (DLP): A category of security controls that prevents the loss or mis disclosure of confidential data.

Workforce: County Employees, contractors, and vendors of San Joaquin County.

POLICY

This policy applies to all employees, contractors, consultants, temporary staff, and other workers at San Joaquin County, including personnel affiliated with third parties, who use their personally owned devices to access the organization’s network, systems, and data. Devices covered under this policy include, but are not limited to, smartphones, tablets, laptops, and any other mobile or computing devices.

1. The connection of any computing device not owned by the County to a County network (except the Public Wi-Fi provided for public use) or computing device is prohibited unless a request has been submitted to and approved by County IT. County workforce

members must sign the County's BYOD Acceptable Use Policy before attaching their personally owned device to a county network.

2. County IT must ensure that any personally owned device attached to the County network utilize the following endpoint security controls: an approved County MDM; authentication, authorization and accounting (AAA); anti-virus and anti-malware, and automated patching and software updates. County IT must configure an MDM solution to enforce compliance with these security controls on personally owned devices.
3. The County authorizes the use of personally owned devices to access County Systems that are accessible from the Internet (e.g. Microsoft 365), but prohibits the storage of County confidential data on such devices unless those devices are configured with DLP and MDM controls managed by County IT.
4. County IT must use its MDM system to remotely wipe confidential data from personally owned devices when such devices are reported to be lost, stolen or otherwise no longer in the possession of the County workforce member. County IT must also remotely wipe confidential data from the personally owned devices of workforce members who are terminated or separate from County service.
5. The loss or theft of a personally owned device must be immediately reported to County IT.
6. Any security incidents involving BYOD devices must be reported and managed in accordance with the County's INCIDENT RESPONSE POLICY SJC-SEC-POL-17.
7. The County reserves right to access personally owned devices containing County confidential data to implement security controls; respond to litigation hold (AKA. e-discovery); fulfill requests arising out of administrative, civil, or criminal directives; investigate Public Record Act requests and subpoenas; or otherwise comply with applicable state or federal laws. Such access will be performed by an authorized technician or designee using a legitimate software process.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County Information Technology (IT) resources, and other actions as well as both civil and criminal penalties

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a timeframe for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

DATE ISSUED/DATE REVIEWED

Date Issued:	04/14/2025
Date Reviewed:	03/11/2026

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53 – Personal Owned Device (SR), NIST CSF 2.0 GOVERN(GV). OV-01, ISO/IEC 27001:2022, NIST SP 800-63, NIST SP 800-66, HIPAA Security Rule; Federal Information Processing Standards (FIPS) 140-2, FIPS 197, FIPS 201

Policy #:	Title:	Effective Date:
SJC-SEC-POL-3	Workstation Use and Security Policy	12/01/2023

PURPOSE

To ensure that County Departments implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access confidential data (e.g., electronic protected health information (ePHI)), to restrict access to authorized users.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. WORKSTATION CONTROLS

County IT shall (or other staff as applicable):

- a. Implement physical and technical safeguards for all workstations that access confidential data (e.g., ePHI) to restrict access to authorized users;
- b. Restrict physical access to workstations to only authorized personnel;
- c. Prevent unauthorized access to a workstation by initiating a session lock after 30 minutes of inactivity or upon receiving a request from a user (see ACCESS CONTROL POLICY);
- d. Configure a password-protected screen saver to ensure that workstations that were left unsecured will be protected;
- e. Restrict non-privileged users from installing software on workstations;
- f. Configure workstations to store confidential data (e.g., ePHI) on data center servers and not on workstation storage media;
- g. Encrypt the storage media of workstations that are used to access confidential data (e.g., ePHI) per County standards;
- h. Use screen protectors on workstations (but not including laptop displays) in public or shared spaces that access confidential data (e.g., ePHI);
- i. Configure and deploy workstations from a secure baseline (see CONFIGURATION MANAGEMENT POLICY).

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests. confer with the requesting County Department.

DATE ISSUED/DATE REVIEWED

Date Issued:	12/01/2023
Date Reviewed:	03/11/2026

REFERENCE

HIPAA Security Rule: Workstation Use and Security: 45 CFR 164.310.(b and c)

Policy #:	Title:	Effective Date:
SJC-SEC-POL-4	Identification and Authentication Policy	12/01/2023

PURPOSE

To ensure that only properly identified and authenticated users and devices are granted access to County Information Technology (IT) resources in compliance with County IT security policies, standards, and procedures.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. IDENTIFICATION AND AUTHENTICATION

County IT shall:

- a. Ensure that information systems uniquely identify and authenticate County users or processes acting on behalf of County users.
- b. Ensure that information systems implement multifactor authentication for system access by privileged accounts, or as required by federal and state laws and regulations governing the management of any confidential data contained in such systems (e.g., electronic protected health information (ePHI));
- c. Ensure that information systems implement multifactor authentication for remote access to county networks by users and devices connecting from non-county networks;
- d. Ensure that websites or information systems containing confidential information (e.g., ePHI) and operating outside of county facilities implement multifactor authentication.
- e. Ensure that information systems implement multifactor authentication for remote access to privileged and non-privileged accounts so that one of the factors is provided by a device separate from the system gaining access and the device utilizes cryptographic mechanisms that protect the primary authentication token (secret key, private key or one-time password) against compromise by protocol threats including: eavesdropper, replay, online guessing, verifier impersonation and man-in-the-middle attacks.

2. DEVICE IDENTIFICATION AND AUTHENTICATION

County IT shall:

- a. Ensure that information systems uniquely identify and authenticate all devices before establishing a network connection. See SJC-SEC-POL-XX “ASSET MANAGEMENT POLICY” for device identification guidelines.

3. IDENTIFIER MANAGEMENT

County IT shall:

- a. Ensure that the County manages information system identifiers by receiving authorization from Human Resources (HR) and/or reporting manager to assign an individual, group, role, or device identifier.
- b. Select an identifier that identifies an individual, group, role, or device;
- c. Assign the identifier to the intended individual, group, role, or device;
- d. Prevent reuse of identifiers; and
- e. Disable the identifier after 90 days of inactivity unless authorized by department head.

4. AUTHENTICATOR MANAGEMENT

County IT shall (or other staff as applicable):

- a. Manage information system authenticators by verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator.
- b. Establish and implement administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.
- c. Ensure that information systems for password-based authentication enforce minimum password complexity for standard user accounts, specifically that passwords meet the following requirements:
 - i. Require passwords to have a minimum length of 15 characters for single factor authentication. When combined with Multi-Factor Authentication (MFA), passwords must be **at least 8 characters**. Must always follow latest [NIST guideline](#)
 - ii. Restrict passwords from containing the user’s account name, username, or display name.
 - iii. Prohibit passwords that appear on a list of commonly used, weak, or compromised passwords per County standards (e.g., breached password blocklists).

- iv. Do not require passwords to comply with additional complexity requirements such as special characters, numbers, or mixed cases.
- d. Ensure that information systems with administrative, system or privileged accounts using password-based authentication enforce the following password complexity requirements:
 - i. Require passwords to have a minimum length of either 20 characters or the maximum length the system will allow.
 - ii. Restrict passwords from containing the user's account name, username, or display name.
 - iii. Prohibit passwords that appear on a list of commonly used, weak, or compromised passwords per County standards (e.g., breached password blocklists).
 - iv. Do not require passwords to comply with additional complexity requirements such as special characters, numbers, or mixed cases.
- e. Require users of non-privileged accounts to change their passwords immediately upon detection of compromise, but do not require users to change their passwords on a predetermined schedule (i.e. password rotation).
- f. Configure Privileged Account Management (PAM) systems and Active Directory to change the passwords of service accounts and share generic privileged accounts after each use, or no less frequently than every 30 days.
- g. Manage accounts that control system processes (i.e. service accounts) with the following additional controls:
 - i. Grant the minimum privileges necessary per vendor or manufacturer specifications for the service account to perform its role or function;
 - ii. For service accounts in a Microsoft Active Directory, configure as Microsoft "Managed Service Accounts" (MSAs);
 - iii. Otherwise, if a service account cannot be managed as an MSA, configure as a non-interactive account and manage its password in a Privileged Account Management (PAM) system per County standards.

- h. Manage privileged shared accounts (e.g. Active Directory “Enterprise Administrator”) in a Privileged Account Management (PAM) system per County standards.
- i. Train users to pick unique and diverse passwords, avoid common password algorithms, use multi-factor authentication wherever possible, and prohibit users from saving their passwords in cleartext.
- j. Store and transmit only cryptographically protected passwords, and do not store passwords using reversible encryption.
- k. Passwords must be protected using strong hashing, salting, and stretching algorithms (e.g., modern adaptive hashing).
- l. Prohibit password reuse for 10 generations.
- m. Allow the use of temporary passwords for initial system logons with an immediate change to a permanent password.
- n. Ensure that information system, for PKI-based authentication, validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.
- o. Require that the registration process to receive specific authenticators (as password) be conducted in person or by a trusted/vetted third party solution; and
- p. Ensure that the information system for hardware/software token-based authentication complies with County standards.
- q. Require that users with multiple identifiers, including staff with separate privileged or administrative accounts, use separate, unique passwords for each of their accounts.
- r. At least, annually, test the strength of users’ passwords stored in Active Directory by using an approved password auditing or breached password detection solution. Require immediate password resets for all accounts found to be non-compliant.

5. CRYPTOGRAPHIC MODULE AUTHENTICATION

County IT shall:

- a. Ensure that information systems implement mechanisms for authentication to a cryptographic module that meet the requirements of applicable state and federal laws, directives, policies, regulations, standards, and guidance for such authentication.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

DATE ISSUED/DATE REVIEWED

Date Issued:	04/15/2020
Date Reviewed:	03/11/2026

REFERENCE

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53a – Identification and Authentication (IA), NIST SP 800-12, NIST SP 800-63, NIST SP 800-73, NIST SP 800-76, NIST SP 800-78, NIST SP 800-100, NIST SP 800-116;
Homeland Security Presidential Directive (HSPD) 12 Policy for a Common Identification Standard for Federal Employees and Contractors;
Federal Information Processing Standards (FIPS): FIPS 201, FIPS 140;
State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.
HIPAA Security Rule: Unique User Identification: 45 CFR 164.312.(a)(2)(i)
HIPAA Security Rule: Person or Entity Authentication: 45 CFR 164.312.(d)

Policy #:	Title:	Effective Date:
SJC-SEC-POL-5	Auditing and Accountability Policy	12/01/2023

PURPOSE

To ensure that County Information Technology (IT) resources and information systems are established with effective security controls and control enhancements that reflect applicable federal and state laws, Executive Orders, directives, regulations, policies, standards, and guidance.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. AUDIT EVENTS

County IT shall:

- a. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use confidential data (e.g., ePHI). Specifically, audit logs must be configured to capture the following activity:
 - i. User log-in events and authentication attempts including user identifying information, timestamps, authentication successes and failures, and password updates;
 - ii. Information about devices used to access systems with confidential data (e.g., ePHI) including timestamps, device names and device IP addresses; and
 - iii. Application activity within information systems that contain confidential data (e.g., ePHI) including creation, modification, and deletion of confidential data records.
- b. Record all events related to the creation, modification, or deletion of privileged or system administrator accounts.
- c. Aggregate and report security-related system and application events to a Security Incident and Event Management (SIEM) system.

2. REVIEWS AND UPDATES

County IT shall (or other staff as applicable):

- a. Perform a user activity review for all systems that contain confidential data (e.g., ePHI) at least quarterly to monitor and detect potentially malicious user behavior.

Monitor for indications of inappropriate data access, credential theft and other insider attacks.

- b. Monitor and review all events related to the creation, modification, or deletion of privileged or system administrator accounts within 1 business day. Respond and investigate any inappropriate or unauthorized privileged account activity upon detection.
- c. Monitor and detect anomalies and respond as per County policy and departmental procedures (See INCIDENT RESPONSE POLICY and CYBERCRIME AND RANSOMWARE INCIDENT RESPONSE POLICY)

3. AUDIT STORAGE CAPACITY AND AUDIT RECORD RETENTION

County IT shall:

- a. Provision audit record storage capacity sufficient to retain audit logs for 1 year or as required by federal or state laws or regulations that govern the data contained within the information systems.

4. TRANSFER TO ALTERNATE STORAGE

County IT shall:

- a. Off-load audit records immediately onto a different system or media than the system being audited.

5. PROTECTION OF AUDIT INFORMATION

County IT shall:

- a. Protect audit information and audit tools from unauthorized access, modification, and deletion.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a period for

achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

DATE ISSUED/DATE REVIEWED

Date Issued:	04/15/2020
Date Reviewed:	03/11/2026

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Auditing and Accountability (AU), NIST SP 800-12, NIST SP 800-92, NIST SP 800-100;

State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.

HIPAA Security Rule: Audit Controls: 45 CFR 164.312.(b)

HIPAA Security Rule: Information System Activity Review: 45 CFR 164.308.(a)(1)(ii)(D)

Policy #:	Title:	Effective Date:
SJC-SEC-POL-6	Configuration Management Policy	12/01/2023

PURPOSE

To ensure that County Information Technology (IT) resources are inventoried and configured in compliance with County IT security policies, standards, and procedures.

DEFINITION

baseline configuration—a representation of the settings, software, and state of a CI, that is formally reviewed and agreed to at a given point in time and can only be modified through a formal CCM process. The baseline is used as a reference to manage the integrity of a CI over its lifecycle.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. BASELINE CONFIGURATION

County IT shall:

- a. Implement and maintain a configuration management system per County standards.
- b. Develop, document, and maintain under configuration control, baseline configurations of information systems in compliance with County standards.
- c. Review and update baseline configurations of information systems at least annually.
- d. Retain one previous version of baseline configurations of information systems to support rollback.

2. CONFIGURATION CHANGE CONTROL

County IT shall:

- a. Continuously monitor information systems for changes or discrepancies against baseline configurations. Review and remediate as appropriate.
- b. Each department shall develop a formal change control procedure that outlines the process to be used for identifying, classifying, approving, implementing, testing, and documenting changes to its IT resources.

- c. Review proposed configuration-controlled changes to the information system and approve or disapprove such changes in accordance with County policies and standards (see MAINTENANCE POLICY).
- d. Coordinate and provide oversight for configuration change control activities through a change advisory board in accordance with County policies and standards (see MAINTENANCE POLICY).

3. SOFTWARE USAGE RESTRICTIONS

County IT shall:

- a. Use software and associated documentation in accordance with contract agreements and copyright laws.
- b. Track the use of software protected by quantity licenses to control copying and distribution.

4. USER-INSTALLED SOFTWARE

County IT shall:

- a. Restrict or prohibit the installation of software by users.
- b. Enforce software installation policies through controlling privileged access and blocking the execution of files using policy applied by directory service and/or application whitelisting.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

DATE ISSUED/DATE REVIEWED

Date Issued:	04/15/2020
Date Reviewed:	03/11/2026

REFERENCE

National Institute of Standards and Technology (NIST) Special Publication (SP): NIST SP 800-53a – Configuration Management (CM);
State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.

Policy #:	Title:	Effective Date:
SJC-SEC-POL-7	Asset Management Policy	04/14/2025

PURPOSE

To establish a framework for the lifecycle management of hardware, software, applications and data assets across the County. This policy aims to ensure that all assets are accounted for, managed, and protected to maintain the confidentiality, integrity, and availability of the organization's information systems and resources.

DEFINITION

Assets: refers to a hardware or software that helps the organization run its operations.

Hardware Assets: are physical devices used in the environment and are tangible information system components required for computing, networking, storage and data processing. These assets fall into various categories as listed below and can exist in physical, virtual or cloud-based environments, including those that can be connected to remotely.

- a. End User\Computing Devices: such as desktops, laptops, tablets, smartphones, desk phones and workstation used for day-to-day operations.
- b. Network devices, such as wireless access points, switches, firewalls, physical/virtual gateways, and routers
- c. Non-computing/Internet of Things (IoT) devices, such as Industrial Control Systems (ICS), HVAC system, security cameras, smart screens, printers, physical security sensors, and IT security sensors
- d. Servers and Storage, such as web servers, SAN\NAS, email servers, application servers, and file servers.

Software Assets: are intangible resources that provide specific functionality and capabilities to perform tasks, manage operations, and achieve business objectives. Some of key examples of software assets:

- a. Operating System (OS): software that manages hardware resources to provide services for other applications (e.g. Windows, Linux, macOS)
- a. Applications: designed for end users to perform specific tasks. Examples include Microsoft Office, Adobe, ERP and CRM and any custom-developed software.

- b. Databases: Database management systems like SQL Server, Oracle, and NoSQL databases like MongoDB.
- c. Security Software: Antivirus programs, endpoint protection platforms, firewalls, and SIEM (Security Information and Event Management) solutions.
- d. Cloud-based Services: Software-as-a-Service (SaaS) applications like Office 365, cloud storage (e.g., AWS S3, Google Cloud Storage), and Infrastructure-as-a-Service (IaaS) solutions.

POLICY

This policy is applicable to all departments and users of County resources and assets.

1. ASSET INVENTORY & ACCOUNTABILITY

County IT shall (or other staff as applicable):

- a. Must identify and maintain inventory of County managed assets that connect to County network resources or process, store, or transmit County data including but not limited to computing devices, network devices, non-computing devices, Telecommunication devices, Servers, Software Internet of things (IoT) and OT devices in an official Asset Management system.
- b. Must adopt a standard naming convention for assets that, at a minimum, includes following:
 - i. Department (see Appendix C: Department Listing)
 - ii. Facility
 - iii. Asset Type (see Appendix D: Device type listing)
- c. Each asset must be assigned a unique asset ID, the following information must be documented in inventory management system for each asset, if applicable:
 - Asset Type
 - Asset Name
 - Asset Supplier/Vendor Name
 - Asset Owning Account/Department
 - Asset Owner
 - Model
 - Serial Number
 - Service Tag - The organization-defined tag for the asset
 - Description of business function
 - Acquisition date

- Status - The status of the asset (such as new, in use, inventory, retired, stolen/missing or retired).
- Location - The actual/physical location of the asset.
- Operating System and OS Version
- VLAN, IP and MAC Address
- Data Sensitivity (e.g. Confidential, restricted, public, ePHI, PII, CJI, PCI) (Refer to SJC-SEC-POL-X “Data Classification Policy” for guidelines)
- Expected Replacement Date/Warranty Expiration Data - The date that the asset is expected to be replaced.
- Licensing Information, including any specific license keys

d. Must audit asset inventory at least annually or real time as change occurs (Adds/moves and changes) for missing data elements (e.g. asset owner, department owner or location) and perform regular reconciliations between physical and logical inventories to ensure consistency.

e. Must remove unauthorized asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset unless temporary access is granted by the department IT.

2. ASSET PROTECTION, SECURITY CONTROLS and CONFIGURATION

County IT shall:

- i. Ensure that only required access is given to assets based on user roles and least privilege in accordance with SJC-SEC-POL-1 “Access Control Policy”
- ii. Apply security controls/updates and endpoint detection and response solution in accordance with SJC-SEC-POL-19 “Data Classification Policy” and SJC-SEC-POL-9 “Information System Integrity Policy”
- iii. All changes to asset configurations or status, including deployment, modification, and decommissioning, must follow the SJC-SEC-POL-14 “Configuration management Policy” and SJC-SEC-POL-1” Maintenance Policy”.

3. ASSET DESTRUCTION, DISPOSAL and REUSE

County IT shall:

- a. All County staff must return assets to be decommissioned or retired or upgraded to County IT department.
- b. Ensure that all information assets are properly stored and /destroyed and/or erased when no longer needed in accordance with SJC-SEC-POL-2 “Media Protection Policy”

- c. All County staff must immediately report lost or stolen county assigned assets to the department IT Service desk.
- d. Must file report with law enforcement for all assets assumed missing or stolen and create security incident report in ticketing system along with changing the status of asset to “Stolen\Missing”.
- e. If the Lost and stolen asset contains protected and confidential data, IT Security Team must initiate a remote wipe if possible and change passwords and access credentials for any systems or accounts associated with the asset.
- f. If the asset contained confidential or sensitive data, the Security Team must notify the appropriate Asset Data Owner and/or privacy officer to perform a risk assessment, and ensure notification was made to the appropriate external agencies (including law enforcement) or individuals who are impacted by the loss of confidential data.
- g. The IT Security Team must conduct an internal investigation of the circumstances of the loss or theft. This may involve reviewing security footage, interviewing personnel, and analyzing access logs. If the incident involves theft, the Security Team must notify and work with local law enforcement.
- h. The IT Security Team or asset custodian must update the asset record status to “Stolen \ Missing” and clear the asset owner, department owner, and location fields as appropriate.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT

Department, initiatives, actions and a timeframe for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

DATE ISSUED/DATE REVIEWED

Date Issued:	03/11/2026
Date Reviewed:	03/11/2026

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53 – Supply Chain Risk Management (SR), NIST CSF 2.0 GOVERN(GV).OV-01, ISO/IEC 27001:2022, NIST SP 800-63, NIST SP 800-66, HIPAA Security Rule; Federal Information Processing Standards (FIPS) 140-2, FIPS 197, FIPS 201

Policy #:	Title:	Effective Date:
SJC-SEC-POL-8	Physical and Environmental Protection Policy	12/01/2023

PURPOSE

To ensure that County Information Technology (IT) resources are protected by physical and environmental security measures that prevent physical tampering, damage, theft, or unauthorized physical access.

POLICY

This policy is applicable to all County departments that use or maintain information systems.

1. PHYSICAL ACCESS AUTHORIZATIONS

County IT shall (or other staff as applicable):

- a. Develop, approve, and maintain a list of individuals with authorized access to the facilities where the information systems reside.
- b. Authorize access to facilities based on role (e.g. visitor, employee, security personnel, IT administrator, etc.)
- c. Issue authorization credentials for facility access.
- d. Review the access list detailing authorized facility access by individuals and remove individuals from the facility access list when access is no longer required.
- e. Control and validate access to software programs for testing and revision.

2. PHYSICAL ACCESS CONTROL

County IT shall (or other staff as applicable):

- a. Enforce physical access authorizations by verifying individual access authorizations before granting access to the facility.
- b. Control ingress/egress to the facility using (one or more) (physical access control systems/devices (as badge reader)) (and/or) security guards.
- c. Maintain physical access audit logs for facility entry/exit points.

- d. Provide SJ County defined security safeguards (as badge reader/security guards etc) to control access to areas within the facility officially designated as publicly accessible.
- e. Escort visitors and monitor visitor activity in SJ County specified secured areas.
- f. Secure keys, combinations, and other physical access devices.
- g. Inventory SJ County defined physical access devices (as keys, badge readers, key fobs etc) at least annually.

3. ACCESS CONTROL FOR TRANSMISSION MEDIUM

County IT shall (or other staff as applicable):

- a. Control physical access to SJ County defined information system distribution and transmission lines within SJ County facilities using County defined security safeguards (as badge readers/keys etc).

4. ACCESS CONTROL FOR OUTPUT DEVICES

County IT shall (or other staff as applicable):

- a. Control physical access to information system output devices to prevent unauthorized individuals from obtaining the output.

Controlling physical access to output devices includes, for example, placing output devices in locked rooms or other secured areas and allowing access to authorized individuals only, and placing output devices in locations that can be monitored by County personnel. Monitors, printers, copiers, scanners, facsimile machines, and audio devices are examples of information system output devices.

5. MONITORING PHYSICAL ACCESS

County IT shall (or other staff as applicable):

- a. Monitor physical access to the facility where the information system resides to detect and respond to physical security incidents.
- b. Review physical access logs upon occurrence of SJ County defined events or potential indications of events (as confirmed unauthorized access attempt); and coordinate results of reviews and investigations with the organizational incident response capability.

6. VISITOR ACCESS RECORDS

County IT shall (or other staff as applicable):

- a. Maintain visitor access records to facilities which contain information systems with confidential data for 2 years or *as required by law*.

- b. Validate visitor identity by examining government issued identification.
- c. Log the date and time of entry and exit by the visitor to the restricted area.
- d. Review visitor access records periodically or as required by law.

7. POWER EQUIPMENT AND CABLING

County IT shall (or other staff as applicable):

- a. Protect power equipment and power cabling for the information system from damage and destruction.
- b. Determine the types of protection necessary for power equipment and cabling employed at different locations both internal and external to organizational facilities and environments of operation. This includes, for example, generators and power cabling outside of buildings, internal cabling and uninterruptable power sources within an office or data center, and power sources for self-contained entities such as vehicles and satellites.

8. EMERGENCY SHUTOFF

County IT shall (or other staff as applicable):

- a. Provide the capability of shutting off power to the information system or individual system components in emergencies.
- b. Place emergency shutoff switches or devices in to facilitate safe and easy access for personnel; and protect emergency power shutoff capability from unauthorized activation.

9. EMERGENCY POWER

County IT shall (or other staff as applicable):

- a. Provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system; transition of the information system to long-term alternate power in the event of a primary power source loss.
- b. Provide a long-term alternate power supply for the information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.

10. EMERGENCY LIGHTING

County IT shall (or other staff as applicable):

- a. Employ and maintain automatic emergency lighting for the information system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.
- b. Provide emergency lighting for all areas within the facility supporting essential missions and business functions.

11. FIRE PROTECTION

County IT shall (or other staff as applicable):

- a. Employ and maintain fire suppression and detection devices/systems for the information system that are supported by an independent energy source.

This applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors.

12. TEMPERATURE AND HUMIDITY CONTROLS

County IT shall (or other staff as applicable):

- a. Maintain temperature and humidity levels within the facility where the information system resides at SJ County defined acceptable levels (as temperature ~70 F, Humidity ~ 30%).
- b. Monitor temperature and humidity levels continuously to include alarms or notifications of changes potentially harmful to personnel or equipment.

13. WATER DAMAGE PROTECTION

County IT shall (or other staff as applicable):

- a. Protect the information system from damage resulting from water leakage by providing master shutoff or isolation valves that are accessible, working properly, and known to key personnel.

This applies primarily to facilities containing concentrations of information system resources including, for example, data centers, server rooms, and mainframe computer rooms. Isolation valves can be employed in addition to or in lieu of master shutoff valves to shut off water supplies in specific areas of concern, without affecting entire organizations.

14. DELIVERY AND REMOVAL

County IT shall (or other staff as applicable):

- a. Authorize, monitor, and control entering and exiting the facility and maintain records of those items delivered and removed from facility.

Effectively enforcing authorizations for entry and exit of information system components may require restricting access to delivery areas and possibly isolating the areas from the information system and media libraries.

15. ALTERNATE WORK SITE

County IT shall (or other staff as applicable):

- a. Employ SJ County defined security controls (as VPN for remote virtual connection etc) at alternate work sites.
- b. Assess as feasible, the effectiveness of security controls at alternate work sites.
- c. Provide a means for employees to communicate with information security personnel in case of security incidents or problems.

Alternate work sites may include, for example, other government facilities or private residences of employees. While commonly distinct from alternative processing sites, alternate work sites may provide readily available alternate locations as part of contingency operations. County staff may define different sets of security controls for specific alternate work sites or types of sites depending on the work-related activities conducted at those sites.

16. CONTINGENCY OPERATIONS

County IT shall (or other staff as applicable):

- a. Establish and implement procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. These procedures must:
 - i. Describe how authorized staff are to access the facility in the event of an emergency;
 - ii. Identify individuals or roles who are authorized to access the facility in the event of an emergency;
 - iii. Be referenced or contained within the department contingency plans.

17. MAINTENANCE RECORDS

County IT shall (or other staff as applicable):

- a. Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example,

hardware, walls, doors and locks). The policies and procedures must, at a minimum address:

- i. How the department documents repairs and modifications to the physical components of its facilities which are related to security;
- ii. Which physical security components require documentation of maintenance activity.
- iii. Special circumstances which may require modifications to physical security components, such as the termination of users with privileged system or physical security access.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

DATE ISSUED/DATE REVIEWED

Date Issued:	04/15/2020
Date Reviewed:	03/11/2026

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Physical and Environmental Protection (PE), NIST SP 800-46, NIST SP 800-73, SP NIST 800-76, SP NIST 800-78, SP NIST 800-116;

Intelligence Community Directive (ICD): 704 705;
Department of Defense (DoD): Instruction 5200.39 Critical Program Information (CPI) Protection;
Federal Identity, Credential, and Access Management (FICAM) publication: Personal Identity Verification (PIV) in Enterprise Access Control System (E-PACS) (2012);
State of California: State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.
HIPAA Security Rule: Facility Access Controls: 45 CFR 164.310(a)(1)

Policy #:	Title:	Effective Date:
SJC-SEC-POL-9	Facility Access Control Policy	12/01/2023

PURPOSE

To ensure that County departments limit physical access to electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed.

POLICY

This policy is applicable to all County departments that store or process confidential data such as electronic protected health information (ePHI).

1. FACILITY ACCESS CONTROLS

County IT shall (or other staff as applicable):

- a. Develop and implement policies and procedures that:
 - i. Address allowing authorized and limit unauthorized physical access to information systems and facilities in which they are housed;
 - ii. Identify individuals or roles with authorized access by title and/or job function;
 - iii. Specify the methods used to control physical access such as door locks, electronic access control systems, security officers, or video monitoring.

2. CONTINGENCY OPERATIONS

County IT shall (or other staff as applicable):

- a. Establish and implement procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency. These procedures must:
 - i. Describe how authorized staff are to access the facility in the event of an emergency;
 - ii. Identify individuals or roles who are authorized to access the facility in the event of an emergency;
 - iii. Be referenced to or contained within the department contingency plans.

3. FACILITY SECURITY PLAN

County IT shall (or other staff as applicable):

- a. Establish and implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering and theft. The department's Facility Security Plan must, at a minimum, address the following:
 - i. How the department screens or evaluates persons and workforce members that need access to its facilities which store or process confidential data;
 - ii. The physical controls in place to prevent unauthorized physical access, tampering or theft of information systems or confidential data;
 - iii. The responsibilities of staff in protecting the facility and its confidential data;
 - iv. A requirement to periodically review and update the Facility Security Plan when there are significant changes to the environment.

4. ACCESS CONTROL AND VALIDATION PROCEDURES

County IT shall (or other staff as applicable):

- a. Implement procedures to control and validate a person's access to department facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. These procedures must, at a minimum, address the following:
 - i. Controlling and validating a person's access to departmental facilities based on their role or function, including visitor control;
 - ii. Identify the methods for controlling and validating a person's access to facilities, such as the use of guards, identification badges, and key cards;
 - iii. Identify the methods for validating and controlling access by visitors;
 - iv. A process to periodically review the list of individuals with physical access to sensitive facilities.

5. MAINTENANCE RECORDS

County IT shall (or other staff as applicable):

- a. Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors and locks). The policies and procedures must, at a minimum address:

- i. How the department documents repairs and modifications to the physical components of its facilities which are related to security;
- ii. Which physical security components require documentation of maintenance activity;
- iii. Special circumstances which may require modifications to physical security components, such as the termination of users with privileged system or physical security access.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

DATE ISSUED/DATE REVIEWED

Date Issued:	04/15/2020
Date Updated:	03/11/2026

REFERENCE

HIPAA Security Rule: Facility Access Controls: 45 CFR 164.310(a)(1)
HIPAA Security Rule: Contingency Operations: 45 CFR 164.310(a)(2)(i)
HIPAA Security Rule: Access Control and Validation: 45 CFR 164.310(a)(2)(iii)
HIPAA Security Rule: Maintenance Records: 45 CFR 164.310(a)(2)(iv)

Policy #:	Title:	Effective Date:
SJC-SEC-POL-10	Maintenance Policy	12/01/2023

PURPOSE

To ensure that County Information Technology (IT) resources are maintained in compliance with County IT security policies, standards, and procedures.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

4. CONTROLLED MAINTENANCE

County IT shall:

- a. Create and maintain records of maintenance and repairs on information systems and components.
- b. Monitor all maintenance activities on information systems, whether performed by county employees or contractors.
- c. Use a change management process for all system maintenance activities, including change documentation, testing and an approval process.
- d. Maintain a log of the location and movement of information systems or system components that store confidential data. (See “Data Classification Policy”)
- e. Sanitize equipment to remove all information from associated media prior to removal from county facilities for off-site maintenance or repairs.
- f. Check all potentially affected security controls to verify that the controls are still functioning properly following maintenance or repair actions.

5. MAINTENANCE TOOLS

County IT shall:

- f. Ensure that system owners and County IT approve, control, and monitor information system maintenance tools.
- g. Check media containing diagnostic and test programs for malicious code before the media are used in the information system.

6. NONLOCAL MAINTENANCE

County IT shall:

- a. Approve and monitor non-local maintenance and diagnostic activities.
- b. Employ strong authenticators in the establishment of nonlocal maintenance and diagnostic sessions. (See “Identification and Authentication Policy”)
- c. Maintain records for nonlocal (& local) maintenance and diagnostic activities.
- d. Terminate session and network connections when nonlocal maintenance is completed.

7. MAINTENANCE PERSONNEL

County IT shall:

- a. Establish a process for maintenance personnel authorization and maintain a list of authorized maintenance organizations or personnel.
- b. Designate County personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

8. TIMELY MAINTENANCE

County IT shall:

- a. Obtain maintenance support and/or spare parts for information systems as agreed upon within the service level agreement between IT and the system owner.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation

measures to be undertaken by the County Department, initiatives, actions and a timeframe for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

DATE ISSUED/DATE REVIEWED

Date Issued:	04/15/2020
Date Reviewed:	03/11/2026

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53 – System Maintenance (MA), NIST SP 800-12, NIST SP 800-63, NIST SP 800-88, NIST SP 800-100;
Federal Information Processing Standards (FIPS) 140-2, FIPS 197, FIPS 201;
State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.

Policy #:	Title:	Effective Date:
SJC-SEC-POL-11	Media Protection Policy	12/01/2023

PURPOSE

To ensure that County Information Technology (IT) controls access to and disposes of media resources in compliance with County IT security policies, standards, and procedures.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. MEDIA ACCESS:

County IT shall:

- a. Restrict access to digital (as USB drive etc) and/or non-digital (as paper records created/maintained by County IT) media to only authorized department personnel.

2. MEDIA STORAGE

County IT shall:

- a. Specify staff to physically control and securely store media within defined controlled areas.
- b. Protect information system media which is to be retired until the media are destroyed or sanitized using county approved equipment, techniques, and procedures.

3. MEDIA TRANSPORT

County IT Shall:

- a. Implement procedures that govern the receipt and removal of hardware and electronic media that contains confidential data (e.g. electronic protected health information (ePHI)) into and out of county facilities and within county facilities.
- b. Maintain accountability/integrity/chain of custody for electronic media during transport outside of controlled areas.
- c. Document activities associated with the transport of information system media containing confidential data. A record of the move, including the individual responsible for the security of the confidential data (e.g. ePHI) contained on the hardware or electronic media will be documented.

- d. Restrict the activities associated with the transport of information system media to authorized personnel.

4. MEDIA SANITIZATION

County IT shall:

- a. Sanitize prior to disposal, release out of organizational control, or release for reuse using SJ County specified standard (as degaussing, cryptographic erasure, shred confidential documents etc) in accordance with applicable federal and organizational standards and policies.
- b. For media containing ePHI, sanitize in accordance with Department of Health and Human Services guidance specifying the technologies and methodologies that render protected health information unusable, unreadable, or indecipherable to unauthorized individuals, such that the ePHI cannot be retrieved and render the ePHI “secured” and not subject to the HIPAA Security Breach Notification Requirements.
- c. For media containing other regulated data, employ sanitization mechanisms with the strength and integrity that conforms with the appropriate law or regulation.

5. MEDIA DISPOSAL

County IT shall:

- a. To the extent that disposal of confidential data (e.g. ePHI) is permitted by applicable law, properly dispose of the data and, if necessary, the hardware or electronic media on which it is stored.
- b. Prior to disposal of any electronic media that contains confidential data (e.g. ePHI), sanitize the media per this policy.
- c. Develop and implement procedures to dispose of electronic media in a secure manner, either internally or by a disposal service.
- d. Obtain certificate of destruction\disposal if hardware assets are disposed through an authorized disposal company and disposal certificate must be stored in Asset Management System in asset record

6. MEDIA RE-USE

County IT shall:

- a. Remove confidential data (e.g. ePHI) from all electronic media before it is made available for re-use. Ensure that confidential data (e.g. ePHI) cannot be read or

recovered from the hardware or media made available for re-use.

- b. Prior to re-use of any electronic media that contains confidential data (e.g. ePHI), sanitize the media per this policy.

7. DATA BACK-UP AND STORAGE

County IT shall:

- a. When needed, create a retrievable, exact copy of confidential data (e.g. ePHI) before movement of hardware or electronic media containing such data pursuant to the department's data back-up or protection plan.
- b. Ensure that the data back-up processes function appropriately in accordance with this policy.

8. REMOVABLE MEDIA

County IT shall (or other staff as required):

- a. Prohibit the storage of confidential data (e.g., ePHI) on unencrypted removable media; and
- b. Limit and control the removable media devices that access county data to only authorized devices;
- c. Store confidential data (e.g., ePHI) on removable media, as required, only in encrypted form in accordance with County standards.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for

achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

DATE ISSUED/DATE REVIEWED

Date Issued:	04/15/2020
Date Reviewed:	03/11/2026

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53 – Media Protection (MP), NIST SP 800-12, NIST SP 800-56, NIST SP 800-57, NIST SP 800-60, NIST SP 800-88, NIST SP 800-100, NIST SP 800-111;
NIST Federal Information Processing Standards (FIPS) 199;
State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.
Department of Health and Human Services Guidance to Render Unsecured Protected Health Information Unusable to Unauthorized Individuals

Policy #:	Title:	Effective Date:
SJC-SEC-POL-12	Security Awareness and Training Policy	12/01/2023

PURPOSE

To ensure that the appropriate level of information security awareness training is provided to all County Information Technology (IT) users.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. SECURITY AWARENESS TRAINING

The County shall:

- a. Schedule security awareness training as part of initial training for new users.
- b. Schedule periodic security awareness training when required by information system changes or as need arises but at least yearly.
- c. Determine the appropriate content of security awareness training and security awareness techniques based on the specific organizational requirements and the information systems to which personnel have authorized access. The content shall:
 - i. Include a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents.
 - ii. Address awareness of the need for operations security. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.
 - iii. Include procedures for guarding against, detecting, and reporting malicious software.
 - iv. Include procedures for monitoring log-in attempts and reporting discrepancies.
 - v. Include procedures for creating, changing and safeguarding passwords.

2. SECURITY AWARENESS | INSIDER THREAT

County IT shall:

- a. Include security awareness training on recognizing and reporting potential indicators of insider threat.

3. ROLE-BASED SECURITY TRAINING

County IT shall (or other staff as applicable):

- a. Provide role-based security training to personnel with assigned security roles and responsibilities or privileged system access:
 - i. Before authorizing access to the information system or performing assigned duties.
 - ii. When required by information system changes and alternate year thereafter.

4. PHYSICAL SECURITY CONTROLS

County IT shall (or other staff as applicable):

- a. Provide initial and ongoing training in the employment and operation of physical security controls; physical security controls include, for example, physical access control devices, physical intrusion alarms, monitoring/surveillance equipment, and security guards (deployment and operating procedures).
- b. Identify personnel with specific roles and responsibilities associated with physical security controls requiring specialized training.

5. PRACTICAL EXERCISES

County IT shall:

- a. Provide practical exercises in security training that reinforce training objectives; practical exercises may include, for example, security training for software developers that includes simulated cyber-attacks exploiting common software vulnerabilities (e.g., buffer overflows), or spear/whale phishing attacks targeted at senior leaders/executives. These types of practical exercises help developers better understand the effects of such vulnerabilities and appreciate the need for security coding standards and processes.

6. SUSPICIOUS COMMUNICATIONS AND ANOMALOUS SYSTEM BEHAVIOR

County IT shall:

- a. Provide training to personnel with assigned security roles on how to recognize suspicious communications and anomalous behavior in organizational information systems.

7. SECURITY TRAINING RECORDS

The County shall:

- a. Designate County personnel to document and monitor individual information system security training activities including basic security awareness training and specific information system security training.
- b. Retain individual training records for 2 years.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

DATE ISSUED/DATE REVIEWED

Date Issued:	04/15/2020
Date Reviewed:	03/11/2026

REFERENCES

National Institute of Standards and Technology (NIST) Special Publications: NIST SP 800-53 – Awareness and Training (AT), NIST SP 800-12, NIST SP 800-16, NIST SP 800-50, NIST SP 800-100;
Electronic Code of Federal Regulations (CFR): 5 CFR 930.301;
State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.
HIPAA Security Rule: Security Awareness and Training: 45 CFR 164.308.(a)(5)(i)

Policy #:	Title:	Effective Date:
SJC-SEC-POL-13	Personnel Security Policy	12/01/2023

PURPOSE

To ensure that personnel security safeguards are applied to the access and use of information technology resources and data.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. PERSONNEL SCREENING

County IT shall:

- a. Screen individuals who will become custodians \ administrators of information systems with confidential data (e.g. ePHI) prior to authorizing access to the information systems.
- b. Ensure personnel screening activities reflect applicable state and federal laws, directives, regulations, policies, standards, guidance, and specific criteria established for the protection of the confidential data.
- c. Establish procedures to ensure that workforce members are granted appropriate access to confidential data (e.g. ePHI), and to prevent workforce members who are not so authorized are not able to obtain access to confidential data (e.g. ePHI).

County HR and Department Directors shall:

- a. Screen prospective employees and contractors who will have access to confidential data (e.g. ePHI) prior to adding them to the county’s workforce.

2. WORKFORCE CLEARANCE, AUTHORIZATION AND SUPERVISION

County HR and County IT shall:

- a. Implement procedures for the authorization and\or supervision of workforce members who will work with confidential data (e.g. ePHI) or in locations where it might be accessed.

- i. For those departments covered by HIPAA (see HIPAA HYBRID ENTITY POLICY), such procedures must authorize and monitor access in

accordance with the applicable requirements of the HIPAA Privacy Rule.

- ii. At a minimum, such departmental procedures should identify workforce members by job classification who require access to ePHI, assign them unique IDs, assign those unique IDs to relevant security roles, and then grant access to ePHI based on security roles. Departmental procedures should outline how County IT will monitor workforce member access to ePHI, and report any inappropriate access, use and disclosure of PHI to the Department's Privacy Officer. Departmental procedures should outline how County IT will modify or remove access to ePHI from workforce members who terminate or change job duties or classification.
- b. Implement procedures to determine that the access of workforce members to confidential data (e.g. ePHI) is appropriate.
 - i. For those departments covered by HIPAA (see HIPAA HYBRID ENTITY POLICY), such procedures should evaluate the appropriateness of workforce member access to ePHI in accordance with the applicable requirements of the HIPAA Privacy Rule.
- c. Implement procedures to review on a periodic basis the access of workforce members to confidential data (e.g. ePHI) to determine that the access is appropriate.

3. PERSONNEL TERMINATION

County IT shall (or other staff as applicable):

- a. Disable information system access immediately or at most within 24 hrs upon notification from HR or a Department Director (or designee) of the termination of a workforce member.
- b. Terminate/revoke any authenticators/credentials associated with the workforce member.
- c. Retrieve all security-related County information system-related property.

Information system-related property includes, for example, hardware authentication tokens and system administration technical manuals.

- d. Revoke access to County information and information systems formerly controlled by the terminated individual.
- e. Terminate access to confidential data (e.g. ePHI) upon termination of employment, or other arrangement, for workforce members, or as otherwise determined

necessary in accordance with the WORKFORCE CLEARANCE, AUTHORIZATION AND SUPERVISION procedure described above.

4. PERSONNEL TRANSFER

County IT shall (or other staff as applicable):

- a. Review and confirm ongoing operational need for current logical and physical access authorizations to information systems/facilities when individuals are reassigned or transferred to other positions within the County.
- b. Modify access authorization as needed to correspond with any changes in operational need due to reassignment or transfer.
- c. This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted.
- d. Modify or terminate access to confidential data (e.g. ePHI) when workforce members transfer or as otherwise determined necessary in accordance with the WORKFORCE CLEARANCE, AUTHORIZATION AND SUPERVISION procedure described above.

5. THIRD-PARTY PERSONNEL SECURITY

County IT shall:

- a. Establish and document personnel security requirements including security roles and responsibilities for contractors or third-party personnel who will have access to information systems with confidential data (e.g. ePHI).
- b. Require third-party providers to comply with personnel security policies and procedures established by the County.
- c. Require third-party providers to notify County defined personnel (as department head/manager) of any personnel transfers or terminations of third-party personnel who possess County credentials and/or badges, or who have information system privileges within 24 hours.

Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management.

6. PERSONNEL SANCTIONS

Department Directors and County Human Resources shall:

- a. Employ a formal sanction process for workforce members failing to comply with these Countywide Information Security Policies and procedures. County sanction processes must comply with applicable state and federal laws, directives, regulations, policies, standards, and guidance.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

DATE ISSUED/DATE REVIEWED

Date Issued:	04/15/2020
Date Reviewed:	03/11/2026

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Personnel Security (PS), NIST SP 800-12, NIST SP 800-60, NIST SP 800-73, NIST SP 800-78, NIST SP 800 -100;
Electronic Code of Federal Regulations (CFR): 5 CFR 731.106;
Federal Information Processing Standards (FIPS) 199 and 201;
Intelligence Community Directive (ICD) 704 Personnel Security Standards;
State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.
HIPAA Security Rule (CFR): Sanction Policy: 164.308(a)(1)(ii)(C)
HIPAA Security Rule (CFR): Workforce Security: 164.308(a)(3)(i)
HIPAA Security Rule (CFR): Workforce Clearance Procedure: 164.308(a)(3)(ii)(B)
HIPAA Security Rule (CFR): Termination Procedures: 164.308(a)(3)(ii)(C)

Policy #:	Title:	Effective Date:
SJC-SEC-POL-14	Risk Management Policy	12/01/2023

PURPOSE

To ensure that County Information Technology (IT) implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. SECURITY MEASURE IMPLEMENTATION

County IT shall:

- a. Based on the periodic assessment conducted as part of the risk analysis (see Risk Assessment Policy), implement security measures that reduce the impact of the threats by reducing the amount and scope of the vulnerabilities. The security measures must:
 - i. Ensure the confidentiality, integrity and availability of all confidential data (e.g. ePHI) that the county creates, receives, maintains, or transmits;
 - ii. Protect against reasonably anticipated threats or hazards to the security or integrity of confidential data (e.g. ePHI); and
 - iii. Ensure compliance with laws and regulations that govern confidential data (e.g. ePHI) by the workforce.
- b. At a minimum the security measures should address the following:
 - i. Restrict access to the confidential data (e.g. ePHI) to only authorized workforce members;
 - ii. Provide periodic training to workforce members on the laws and regulations governing the management of the confidential data (e.g. ePHI);
 - iii. Report and sanction a workforce member who breaches an information security policy or procedure related to the management of confidential data (e.g. ePHI);
 - iv. Periodic risk assessments and reviews of existing security measures;

- v. Ongoing development and implementation of security measures as documented in the department’s Risk Management Plan;
- vi. Password security measures in compliance with the Identification and Authentication Policy;
- vii. Workstation security measures in compliance with the Workstation Use and Security Policy.

2. SECURITY MEASURE DOCUMENTATION

County IT shall:

- a. Document the security measures (including supporting rationale) in a departmental Risk Management Plan.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County Information Technology (IT) resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

DATE ISSUED/DATE REVIEWED

Date Issued:	12/01/2023
Date Reviewed:	03/11/2026

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP):
NIST SP 800-37 Rev. 2 – Risk Management Framework for Information Systems and

Organizations: A System Life Cycle Approach for Security and Privacy
HIPAA Security Rule: Security Management Process: 45 CFR 164.308(a)(1)(ii)(B)

Policy #:	Title:	Effective Date:
SJC-SEC-POL-15	Risk Assessment Policy	12/01/2023

PURPOSE

To ensure that County Information Technology (IT) performs risk assessments in compliance with County IT security policies, standards, and procedures.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. RISK ASSESSMENT

County IT shall (or other staff as applicable):

- a. Conduct (or have conducted by a qualified third-party) an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits, and including the potential risks and vulnerabilities to the confidentiality, integrity and availability of confidential data (e.g. ePHI) held, created, received, maintained, or transmitted by the department. The Risk Assessment must:
 - i. Be updated at least annually, but whenever significant changes are made to business operations or security controls, or whenever significant new threats are detected;
 - ii. Use the NIST Risk Management Framework as the basis of the assessment;
 - iii. Examine the types of threats – internal or external, natural or manmade, electronic and non-electronic – that threaten the confidentiality, integrity and availability of confidential data (e.g., ePHI);
 - iv. Document the existing vulnerabilities which potentially expose the department’s information resources to the threats;
 - v. Evaluate the department’s information assets and technologies for their role and criticality in the processing of confidential data (e.g., ePHI);
 - vi. Determine the impact that would result if a threat were to successfully exploit a vulnerability;

- vii. Evaluate and assess the security controls in place which protect the department's information assets from the identified threats; and
- viii. Estimate the resulting risks to the confidentiality, integrity, and availability of confidential data (e.g., ePHI).

- b. Disseminate Risk Assessment results to stakeholders.
- c. Prepare a Risk Management Plan which documents the measures that will be implemented to eliminate, mitigate, transfer, or accept the identified risks (See RISK MANAGEMENT POLICY).
- d. Present the Risk Assessment and Risk Management Plan to the department's Director or Department Head for their review and acknowledgement.

2. VULNERABILITY SCANNING

County IT shall:

- a. Scan for vulnerabilities in the information system and hosted applications at least quarterly and/or randomly in accordance with County defined process or applicable regulations and when new vulnerabilities potentially affecting the system/applications are identified and reported.
- b. Employ vulnerability scanning tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
 - i. Enumerating platforms, software flaws, and improper configurations.
 - ii. Formatting checklists and test procedures.
 - iii. Measuring vulnerability impact.
- c. Analyze vulnerability scan reports and results from security control assessments.
- d. Remediate all high-risk vulnerabilities within one month of detection in accordance with an organizational assessment of risk. Remediate and reduce the number of medium and low risk vulnerabilities between each quarterly scan.
- e. Employ vulnerability-scanning tools that include the capability to readily update the information system vulnerabilities to be scanned.

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

DATE ISSUED/DATE REVIEWED

Date Issued:	04/15/2020
Date Reviewed:	03/11/2026

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – Risk Assessment (RA), NIST SP 800-12, NIST SP 800-30, NIST SP 800-39, NIST SP 800-40, NIST SP 800-60, NIST SP 800-70, NIST SP 800-100, NIST SP 800-115;
NIST Federal Information Processing Standards (FIPS) 199;
State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.
HIPAA Security Rule: Risk Analysis: 45 CFR 164.308(a)(1)(ii)(A)

Policy #:	Title:	Effective Date:
SJC-SEC-POL-16	Vendor and Third-Party Management	12/01/2023

PURPOSE

To ensure that County Departments and Agencies establish information technology vendor agreements and exchange confidential data (e.g., electronic protected health information (ePHI)) with third parties in compliance with County information security policies and standards.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. Statements of Work

Department Directors shall (or other staff as applicable):

- a. Conduct due diligence of vendors and third parties to ensure they are capable of protecting the County’s confidential data (e.g., ePHI) and that they understand and accept their obligations under County policy and applicable federal and state laws and regulations;
- b. Enter into agreements that clearly state the scope of services provided under the contract, and the information security controls to be used to protect confidential data (e.g., ePHI);
- c. Ensure that agreements include a screening process for contractors or third-party users who will have access to confidential data (e.g., ePHI);
- d. Preferentially enter into agreements with vendors who have been approved by StateRAMP or FedRAMP, or who have received HITRUST certification;
- e. Execute business associate agreements with any third parties who access, store, process or transmit ePHI (see BUSINESS ASSOCIATE AGREEMENTS)

2. Public or Resident Access

County IT shall (or other staff as applicable):

- a. Ensure that the public and county residents are aware of their obligations and rights, and accept the responsibilities and liabilities involved in accessing, processing, communicating, or managing the county’s information and information assets;

- b. Provide appropriate text or a link to the organization's privacy policy for data use by the public or county residents;
 - c. Authenticate public or resident users prior to granting access to any confidential data (e.g., ePHI).
3. Technical Controls
County IT shall (or other staff as applicable):
- a. Configure remote access for third parties and contractors in compliance with County policies and standards (see ACCESS CONTROL POLICY);
 - b. Configure contractor\vendor and temporary accounts with an automatic termination date no greater than 30 days from account creation, or as permitted by contract (e.g., Independent Contractor Agreement);
 - c. Restrict or limit remote access by third parties to the minimum necessary information systems and confidential data (e.g., ePHI) to perform their contractual obligations.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests. confer with the requesting County Department.

DATE ISSUED/DATE REVIEWED

Date Issued:	12/01/2023
Date Reviewed:	03/11/2026

REFERENCE

HITRUST ALLIANCE: <https://hitrustalliance.net/>

StateRAMP Authorized Product: <https://stateramp.org/product-list/>

FedRAMP Marketplace: <https://marketplace.fedramp.gov/products>

Policy #:	Title:	Effective Date:
SJC-SEC-POL-17	Business Associate Agreements	12/01/2023

PURPOSE

To ensure that County Departments and Agencies, where appropriate, enter into Business Associate Agreements with third parties that store, process or transmit electronic protected health information (ePHI) on their behalf.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. Business Associate Agreements
 Department Directors shall (or other staff as applicable):
 - a. Execute a Business Associate Agreement with all Business Associates who create, maintain, access, receive, or transmit ePHI on behalf of County departments;
 - b. Ensure that Business Associate Agreements executed by County departments comply with the requirements of the HIPAA Privacy Rule, the HIPAA Security Rule, the HITECH Act, and County policies and standards;
 - c. Use, wherever possible, San Joaquin County’s Master Business Associate Agreement as the template for any new Business Associate Agreement;
 - d. Retain copies of all signed Business Associate Agreements for a period of at least six (6) years from the date when last in effect
 - e. Maintain an inventory of all Business Associate Agreements executed by County departments.

2. Limitations on Disclosure
 Department Directors shall (or other staff as applicable):
 - a. Permit an individual to request restriction of the disclosure of the individual's covered information to a business associate for purposes of carrying out payment or health care operations, and is not for purposes of carrying out treatment, and respond to any requests from an individual on the disclosure of the individual's covered information.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests. confer with the requesting County Department.

DATE ISSUED/DATE REVIEWED

Date Issued:	12/01/2023
Date Reviewed:	03/11/2026

REFERENCE

HIPAA Security Rule: Business Associate Contracts: 45 CFR 164.308(b)
HIPAA Privacy Rule: Uses and Disclosures of Protected Health Information: 45 CFR 164.502(a)(3)
San Joaquin County Master Business Associates Agreement (see County Counsel)

Policy #:	Title:	Effective Date:
SJC-SEC-POL-18	Information System and Services Acquisition Policy	12/01/2023

PURPOSE

To ensure that County Information Technology (IT) resources and information systems are acquired with security requirements to meet the County information systems mission and business objectives.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. ALLOCATION OF RESOURCES

County IT shall:

- a. Identify all business applications that are used by their users in support of primary business functions. This includes all applications owned and/or managed by the department as well as other business applications that are used by the department but owned and/or managed by other County ISD IT. All business applications used by a department shall be documented in the department’s IT security plan as well as their Business Impact Analysis (BIA).
- b. Determine information security requirements for the information system or information system service in compliance with County Information Security Policies and Standards and any applicable laws and regulations that govern the management of confidential data (e.g. ePHI) managed or processed by the system.
- c. Determine, document, and allocate the resources required to protect the information system or information system service as part of its capital planning and investment control process.

2. SYSTEM DEVELOPMENT LIFE CYCLE(SDLC)

County IT shall:

- a. Manage the information system using a SDLC methodology that includes information security considerations.
- b. Define and document information system security roles and responsibilities throughout the SDLC
- c. Identify individuals having information system security roles and responsibilities; and

- d. Integrate the organizational information security risk management process into SDLC activities.
- e. Custom developed software refers to SJC Policy CUSTOM DEVELOPED SOFTWARE
- f. GUIDELINES for SDLC: Many SDLC models exist that can be used by an organization in developing an information system. A traditional SDLC is a linear sequential model. This model assumes that the system will be delivered near the end of its life cycle. A general SDLC should include the following phases:
 - i. Initiation
 - ii. Acquisition / Development
 - iii. Implementation / Assessment
 - iv. Operations / Maintenance
 - v. Sunset
- g. Each of these five phases should include a minimum set of tasks to incorporate security in the system development process. Including security early in the SDLC will usually result in less expensive and more effective security than retrofitting security into an operational system.
- h. The following questions should be addressed in determining the security controls that will be required for a system:
 - i. How critical is the system in meeting the organization's mission?
 - ii. What are the security objectives required by the system, e.g., integrity, confidentiality, and availability?
 - iii. What regulations, statutes, and policies are applicable in determining what is to be protected?
 - iv. What are the threats that are applicable in the environment where the system will be operational?
 - v. What kinds of data will be used by the system?

3. ACQUISITION PROCESS

County IT shall:

- b. Acquire systems that comply with County Information Security Policies and Standards;

- c. Ensure the acquisition process includes the following requirements, descriptions, and criteria, explicitly or by reference, in the acquisition contract for the information system, system component, or information system service in accordance with applicable federal, state, and local laws, Executive Orders, directives, policies, regulations, standards, guidelines, and County mission and business needs:
 - i. Security and privacy functional requirements shall include security capabilities, security functions, and security mechanisms.
 - ii. Security assurance requirements shall include following:
 - a. Development processes, procedures, practices, and methodologies.
 - b. Evidence from development and assessment activities providing grounds for confidence that the required security and/or privacy functionality has been implemented and the required security strength has been achieved.
 - iii. Data sharing or processing agreements where applicable (e.g. HIPAA Business Associate Agreement); and
 - iv. Security-related documentation requirements
 - v. Description of the information system development environment in which the system is intended to operate; and
 - vi. Acceptance criteria.

4. INFORMATION SYSTEM DOCUMENTATION

County IT shall:

- a. Obtain administrator documentation for the information system, system component, or information system service that describes:
 - i. Secure configuration, installation, and operation of the system, component, or service.
 - ii. Effective use and maintenance of security functions/mechanisms.
 - iii. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions.
- b. Obtain user documentation for the information system, system component, or information system service that describes:

- i. User-accessible security functions/mechanisms and how to effectively use those security functions/mechanisms.
- ii. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner.
- iii. User responsibilities in maintaining the security of the system, component, or service.
- iv. Document attempts to obtain information system, system component, or information system service documentation when such documentation is either unavailable or nonexistent (due to the age of the system or lack of support from the vendor or manufacturer) and provide appropriate compensating controls in response.
- v. Protect documentation as required, in accordance with the risk management strategy; and
- vi. Distribute documentation to authorized system personnel

5. SECURITY ENGINEERING PRINCIPLES

County IT shall:

- a. Information system security engineering principles must be applied in the specification, design, development, implementation, and modification of the information system:
- b. Asset custodians are required to implement configuration standards for all system components that address known security vulnerabilities and are consistent with industry-accepted system hardening standards which are CIS Level 1 baseline standards and configuration.
- c. NIST SP 800-160, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems shall be used as guidance on engineering principles for information system security. NIST SP 800-160 may be found at the following link:

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v1.pdf>

6. EXTERNAL INFORMATION SYSTEM SERVICES

County IT shall:

- d. Conducts an organizational assessment of risk prior to the acquisition or outsourcing of services as per SJC-SEC-POL-16 VENDOR AND THIRD PARTY RISK MANAGEMENT policy.
- e. Information Maintains and implements policies and procedures to manage service providers (e.g., Software-as-a-Service (SaaS), Web hosting companies, collection providers, or email providers), through observation, review of policies and procedures, and review of supporting documentation. Including:
 - i. Maintaining a list of service providers.
 - ii. Maintaining a written agreement that includes an acknowledgment that the service providers are responsible for the security of data the service providers possess.
 - iii. Ensuring there is an established process for engaging service providers including proper due diligence prior to engagement.
- f. Maintains a program to monitor service providers' control compliance status at least annually.
- g. Requires that providers of external system services comply with organizational information security requirements and employ appropriate security controls in accordance with local, state and Federal laws, as well as all applicable regulatory requirements.
- h. Defines and documents oversight and user roles and responsibilities regarding external system services; and
- i. Conducts an organizational assessment of risk prior to the acquisition or outsourcing of services.

Asset custodians and data/process owners are required to:

- i. Maintain a comprehensive list of service providers, including all applicable Service Level Agreements (SLAs);
- ii. Require that providers of external systems comply with SJC information security requirements and employ appropriate security controls in accordance with local, state and Federal laws, as well as all applicable regulatory requirements.
- iii. Define oversight responsibilities regarding external system services.
- iv. Perform a review of the service provided for acceptable service levels.
- v. Conduct a risk assessment outsourcing of services; and
- vi. Monitor security control compliance by external service providers.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

DATE ISSUED/DATE REVIEWED

Date Issued:	04/15/2020
Date Reviewed:	03/11/2026

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – System and Services Acquisition (SA), NIST CSF PR.IP-2, NIST CSF ID.RA-1, PCI DSS 2.2 | NIST CSF PR.IP-2, NIST SP 800-12, NIST SP 800-23, NIST SP 800-35, NIST SP 800-36, NIST SP 800-37, NIST SP 800-64, NIST SP 800-65, NIST SP 800-70, NIST SP 800-100, NIST SP 800-128, NIST SP 800-137;

HIPAA 164.308(a)(2)(a). 164.308(a)(4)(a) & 164.314(a), HIPAA 164.308(b)(a), 164.314(a)(1)(i)-(ii), 164.314(a)(1)(ii)(A)-(B), 164.314 (a)(2)(i)(A)-(D), 164.314(a)(2)(i)(A)-(D), 164.314(a)(2)(ii)(a)-(b) | PCI DSS 2.6 & 12.9, HIPAA 164.314(b)(a)-(b) | PCI DSS 12.9

Homeland Security Presidential Directive (HSPD) 12;
International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) Standard 15408;
State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.

Policy #:	Title:	Effective Date:
SJC-SEC-POL-19	Custom Developed Software Policy	04/14/2025

PURPOSE

Custom developed software, while often tailored to meet department needs, is considered a high-risk endeavor within the County due to potential risks on information security and the significant financial investment required for development and maintenance. For these reasons, our approach to adding software to our portfolio is guided by a strategic prioritization scheme:

1. Software as a Service (SaaS)
2. Commercial Off-The-Shelf Software (COTS)
3. Systems built on Platform as a Service (PaaS) solutions
4. Custom Developed Software

Custom software is placed at the lowest priority because it not only introduces inherent security risks due to its custom-made nature, but also incurs greater costs over time in comparison to SaaS or COTS options. Furthermore, Custom solutions can become difficult to scale or adapt to changing business needs, often resulting in technical debt and system obsolescence over time. This can hinder the organization’s ability to respond to new opportunities and challenges

Given these challenges, custom development should only be considered when all other solutions (SaaS, COTS and PaaS) are unable to meet County’s\Agencies specific requirements and when a strong business case justifies its necessity. This approach will ensure that our technology investments are aligned with best practices for security, cost management, operational efficiency and financial stewardship, while minimizing the risks associated with custom software development.

This policy will establish security and compliance requirements for development, acquisition, user and management of custom-developed software across all County departments.

This policy ensures that all custom- developed software adheres to secure development practices, minimizes security risks, and complies with applicable regulations and standards.

DEFINITION

Code - refers to the set of instructions or programming language syntax written by developers to create software that performs specific tasks or functions.

Application\Software - term has been used interchangeable throughout this policy but holds same meaning. It is program or set of programs designed to perform specific tasks or functions for users or systems.

Custom-developed software - refers to applications or systems that are specifically designed and built to meet unique business requirements, tailored functionalities, and organizational needs, as opposed to off-the-shelf software solutions.

Software Development Life Cycle (SDLC) - is referred as a structured process used to design, develop, test, and deploy software with security and quality integrated throughout each phase.

Software development Security Framework (SSDF) - is referred as structured approach that integrate security practices and controls throughout the entire SDLC to ensure protection against vulnerabilities and compliance with security standards.

SQL injection – is referred to as a code injection technique that allows attackers to manipulate SQL queries and gain unauthorized access to or manipulate the database

Cross-Site Scripting (XSS) – is technique used to inject malicious scripts into web pages viewed by other users.

Buffer Overflows – Buffer means memory and Buffer Overflows refers to when more data is written to a buffer than it can hold, leading to potential memory corruption, crashes, or enabling attackers to execute arbitrary code

Software as a Service (SaaS) - A cloud-based software delivery model where applications are hosted by a service provider and accessed over the internet, eliminating the need for local installation and maintenance.

Commercial Off-The-Shelf Software (COTS) - Pre-built software products available for purchase by the public, designed to meet common business needs without requiring custom development.

Software built on Platform as a Service (PaaS) - Cloud-based platforms that provide a framework and tools for developers to build, deploy, and manage applications without managing underlying infrastructure

POLICY

This policy is applicable to all County departments, agencies and users of County resources and assets. It also includes applications\software developed internally, by third-party vendors, or through collaborations with external partners.

1. INITIATION REQUIREMENTS

County IT Agencies shall (or other staff as applicable):

- a. All custom software development must follow an established Software Development Life Cycle (SDLC) process which includes security as a fundamental component. Custom software development led by County IT Agencies must follow NIST SP 800-218 secure software development security framework. Other SSDF which can be referred are OWASP SDLC , ISO/IEC 27024, and CIS Controls.
- b. Engage Designated Information Security Officer (DISO) and/or County ISO during the planning phase of new custom developed software and/or changes to existing custom-developed software to define security requirements and ensure they are incorporated into software design, development, testing, and deployment stages
- c. Designated Information Security Officer (DISO) must conduct security risk assessments during both planning and development phase of new custom developed software and third-party vendor(s). This assessment must identify and evaluate potential security risks, vulnerabilities and threats associated with the software. Any high-risk vulnerabilities must be mitigated before the software is approved to go to production. See County Information Security Policy - SJC-SEC-POL-5 RISK ASSESSMENT POLICY and SJC-SEC-POL-16 VENDOR AND THIRD-PARTY MANAGEMENT for further standards.
- d. Must apply set of security controls established by NIST SP 800-53 for secure coding practices.
- e. Must adhere to OWASP's Secure Coding Practices and address the SANS Institute's Top 25 Software Errors.
- f. Developer must use OWASP Cheat Sheet to implement various security controls security controls to prevent common vulnerabilities such as SQL injection, Cross-Site Scripting (XSS), Buffer Overflows, Authentication and Authorization Issues.
- g. Use automated tools for static and dynamic code analysis to identify and resolve potential vulnerabilities early in the development process.

2. IDENTIFICATION

County IT Agencies shall (or other staff as applicable)

- a. Maintain an UpToDate inventory of all custom-developed software and review at least annually to whenever new software is introduced. See SJC-SEC-POL-19 DATA CLASSIFICATION POLICY in County Information Security Policy.
- b. Any new custom-developed software must be registered in the County software asset inventory before deployment to production.

3. DATA PROTECTION

County ITAgencies must (or other staff as applicable):

- a. The three operational environments must be established for any custom-developed software Development, Testing and Production. See County Information Security Policy SJC-SEC-POL-8 Information System and Communications Protection Policy
- b. Segregate development, testing and production application environments to reduce the risks of unauthorized access or changes and aid in supporting methodology execution. Access to program source code shall be restricted to authorized personnel and managed using enterprise configuration management and versioning software. See County Information Security Policy SJC-SEC-POL-8 Information System and Communications Protection Policy
- c. Implement strong encryption to protect protected and confidential data at rest and in transit, to ensure the confidentiality and integrity of protected and confidential information. Encryption keys must be managed securely, rotated regularly, and access to keys should be limited to authorized personnel only. Protected and confidential data should never be transmitted or stored in plain text. See County Information Security Policy SJC-SEC-POL-8 Information System and Communications Protection Policy
- d. Implement strong encryptions for all cached or temporary copies of protected and confidential data stored on the server from unauthorized access and purge those temporary working files a soon as they are no longer required.
- e. Implement data retention policies that specify how long data should be retained and ensure automated processes for secure deletion when data is no longer needed. Regularly review stored data and remove any redundant or obsolete information to reduce the risk of exposure.
- f. Implement secure backup configurations to protect data and configuration files. Ensure backup data is encrypted, stored securely, and regularly tested to verify successful restoration and integrity.
- g. Comply with applicable regulatory compliance requirement (E.g. HIPAA, CJIS, GDPR, PCI-DSS) and County Information Security Policy if protected and confidential information is handled by custom-developed software.

4. ACCESS CONTROL AND AUTHORIZATION

County ITAgencies shall (or other staff as applicable):

- a. All custom application production systems must have a role-based access control system to restrict system access privileges to users.
- b. Multi-Factor Authentication (MFA) is required for access to all development and production environments
- c. Systems shall have designated access control administrators who manage system wide privileges for user roles.
- d. Should the access control administrator also be a regular user of the system, they shall have two role-based accounts – one for administrative access and one for user-based access.
- e. Access controls applied to custom-developed software must adhere to the policy provided in County Information Security Policy SJC-SEC-POL-10 ACCESS CONTROL POLICY.

5. SECURE CONFIGURATION AND DEPLOYMENT

County IT Agencies shall (or other staff as applicable):

- a. Development systems must not contain protected and confidential information, shall be populated with test or dummy data
- b. Configure all software systems with secure defaults to minimize exposure to vulnerabilities. Disable unnecessary features, services, and modules, and enable security controls such as logging, encryption, and access restrictions by default. (E.g. Disable auto complete feature on forms to expected to contain protected and confidential information, including authentication, disable client-side caching on pages containing protected and confidential data etc.)
- c. Follow industry standards and best practices (e.g., CIS Benchmarks, NIST guidelines) to harden software configurations. This includes setting strong authentication methods, secure file permissions, and appropriate session management controls.
- d. Use a version control system to track all configuration changes and ensure only approved modifications are applied. Maintain documentation of all configuration baselines and changes to enable auditing and rollback if necessary. See County Information Security Policy- SJC-SEC-POL-14 CONFIGURATION MANAGEMENT POLICY.

- e. Use automated tools (e.g., Infrastructure-as-Code, Configuration Management Systems) for consistent configuration deployment and to minimize human error. Implement automated testing and validation to ensure configurations are applied correctly and securely.
- f. Configure secure communication protocols (e.g., TLS 1.2/1.3) for data transmission and enforce encryption of protected and confidential data. Disable insecure protocols such as SSL, TLS 1.0/1.1, and weak ciphers that may expose the system to interception and data breaches
- g. Apply secure configurations to APIs by enforcing strong authentication and authorization mechanisms, rate limiting, and input validation to prevent attacks such as API abuse, injection, or data exposure.

6. RISK ASSESSMENT AND RISK MANAGEMENT

Designated Information Security Officer (DISO):

- a. Must conduct security risk assessments for all custom developed software whenever significant changes are made to software (e.g. new features, integration, or migrations) or security controls, or whenever significant new threats are detected. See County Information Security Policy - SJC-SEC-POL-5 RISK ASSESSMENT POLICY for further standards.
- b. Based on the periodic assessment conducted as part of the risk analysis (Risk Assessment Policy), implement security measures that reduce the impact of the threats by reducing the amount and scope of the vulnerabilities. See County Information Security Policy - SJC-SEC-POL-6 RISK MANAGEMENT POLICY for further security measures implementation.
- c. Apply latest security patches and updates to keep software configurations up to date. Schedule regular patch management activities to address vulnerabilities in software libraries, dependencies, and configurations. See INFORMATION SYSTEM INTEGRITY POLICY

7. THIRD PARTY SOFTWARE AND LIBRARIES

County IT Agencies shall (or other staff as applicable):

- a. Must assess and review the security posture of any third-party software components or libraries used in custom-developed software.
- b. Ensure that third-party software and libraries are up-to-date and do not contain known vulnerabilities.

- c. Implement processes for tracking and managing third-party dependencies and ensuring that they comply with security and regulatory standards.

8. MONITORING AND LOGGING

County IT Agencies shall (or other staff as applicable):

- a. Monitor custom-developed software using monitoring tools to analyze log data for suspicious patterns or anomalies, triggering alerts for security teams to investigate potential incidents swiftly. (E.g. of monitoring tools are Snyk, Splunk etc.)
- b. Configure custom-developed software to send logging information to County's Security Information and Event Management (SIEM) systems and/or agencies centralized logging solution to aggregate log data based on severity level (E.g. info, warning, error, critical) and type of log (E.g. access, transaction, error or audit)
- c. Conduct regular reviews and analysis of logs to identify potential security incidents, unusual patterns of behavior, or compliance issues, and integrate findings into ongoing risk management efforts.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County Information Technology (IT) resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a timeframe for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

DATE ISSUED/DATE REVIEWED

Date Issued:	04/14/2025
--------------	------------

Date Reviewed: 03/11/2026

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP800-53, NIST SP 800-171(3.1.1 and 3.3.1), ISO\IEC 27024, CIS Controls, SANS (SysAdmin, Audit, Network, and Security Institute) Top 25 Software Errors, OWASP (Open Web Application Security Project) SDLC and Secure coding practices

Policy #:	Title:	Effective Date:
SJC-SEC-POL-20	Generative Artificial Intelligence (AI) Use Policy	04/14/2025

PURPOSE

To establish a policy for the responsible, ethical, and secure use of Artificial Intelligence (AI) as a tool within the County. This Artificial Intelligence Use Policy (“Policy”) outlines Counties requirements with respect to the adoption of various forms of artificial intelligence.

DEFINITIONS

“Artificial intelligence” (AI) means the use of machine learning technology, software, automation, and algorithms to perform tasks and make rules or predictions based on existing datasets and instructions.

“Generative AI Tools” are computer programs capable of many activities, including but not limited to completing general administrative office tasks, data analysis, programming, and image creation.

“Closed AI system” means an AI system where the input provided by one user is used to train the AI model. Input data from the user is isolated from other users, and the data is considered more secure. (e.g. Microsoft 365 Copilot)

“Open AI system” means an AI system where the input provided by all users is used to train the AI model. Input data from all users is not private and may be revealed to other users. (e.g. OpenAI ChatGPT)

POLICY

This policy applies to all County departments and users of County resources and assets, contractors, and third-party individuals who have access to AI technologies or are involved in using AI tools or platforms on behalf of County.

1. ACCEPTABLE USE

- a. GenAI tools may only be used for business purposes approved by the department. Such purposes may include but not limited to:
 - a. Content creation and assistance
 - b. Research and product development
 - c. Analysis of non-sensitive data
 - d. Requesting code examples and programming guidance for non-sensitive applications

- b. AI tools and platforms may only be used for business purposes approved by the department. Such purposes may include content generation for marketing, product development, research, or other legitimate activities.
- c. All users must indicate when Generative AI tool is used for the development of a work product wherever possible. For example, when working with regulatory, legal, or life critical subjects, citations shall be required. When attributing AI usage in a work product indicate the product and version used. Examples include:
 - a. Whole Document example: [AI Assistance: This document was generated with the assistance of an Artificial Intelligence language model, Microsoft 365 Copilot, in compliance with the San Joaquin County Generative AI Use Policy.]
 - b. Specific Citation Example: OpenAI. (2023). ChatGPT (Mar 14 version) [Large language model].
 - c. In text example for specific information: (OpenAI, 2023)
- d. All use of AI must comply with applicable laws, regulations, and ethical guidelines governing intellectual property, including, but not limited to, copyright, privacy, and data protection.
- e. Users must respect and protect intellectual property rights, both internally and externally. Unauthorized use of material subject to copyright protection, or creation of content that infringes on the intellectual property of others, is strictly prohibited.
- f. Users are responsible for ensuring that the generated content produced using AI aligns with the organization's values, ethics, and quality standards. Generated content must not be used if it is inaccurate, misleading, harmful, offensive, and/or discriminatory.
- g. All AI-generated content (writing, datasets, graphs, pictures, etc.) must be thoroughly reviewed by an individual with expertise to evaluate such content for accuracy as well as general proofing and editing.
- h. Assume any information you enter in a generative AI system may be subject to a California Public Records Act (CPRA) request. Since system employees can see entered data, that data is considered “released to the public” for CPRA purposes.

2. PROHIBITED USE

When using GenAI at the County, **DO NOT:**

- a. Use GenAI for any malicious activity.
- b. Enter confidential data, beliefs, gender, sexual orientation, disability status, or any other private details into an open AI system. (See SJC-SEC-POL-19 “DATA CLASSIFICATION POLICY” for further details.)
- c. Use County user credentials, email addresses, or telephone numbers as a login to publicly available GenAI applications without approval by the ISD Director, or Chief Information Security Officer (CISO).
- d. Use AI systems to identify or categorize students, candidates, employees, contractors, or other affiliated entities based on protected class status. Exceptions for specific use cases must be approved by the ISD Director and/or Chief Information Security Officer (CISO).
- e. Enter trade secrets, confidential and regulated or personal data (PII, PHI, CJI, PCI, HIPAA, or any other proprietary) about any county resident, employee etc. into an open AI system.
- f. Misrepresent work generated by a GenAI tool as being your own original work.
- g. Use AI to generate, modify, or debug County systems, applications, or program codes without approval of the ISD Director or Chief Information Security Officer (CISO).
- h. Create text, audio, or visual content that is intended to represent any individual without their explicit approval and consent.
- i. Install Application Programming Interfaces (APIs), plug-ins, connectors, or software related to GenAI systems, without approval by the ISD Director or the Chief Information Security Officer (CISO).
- j. Use GenAI tools to make or help you make employment decisions about applicants or employees, including recruitment, hiring, retention, promotions, transfers, performance monitoring, discipline, demotion, or terminations.

3. PROCUREMENT DUE DILIGENCE AND COMPLIANCE REVIEW

All staff shall:

- a. Engage their department’s DISO before introducing any new AI systems, tools or platforms. The DISO consultation is required to ensure adherence to security policies and alignment with County standards and risk management protocols. Broad questions that should always be considered before the start of using GenAI include:
 - i. What are potential inequities in problem formulation?
 - ii. What are the data inputs?
 - iii. How and when will the solution be implemented and integrated into existing and future processes and delivery of services?
 - iv. Who will be the GenAI team responsible within the program area to monitor, validate and evaluate the GenAI tool?
 - v. How does using the GenAI tool build trust with the end user, including Californians impacted?
 - vi. Is the GenAI tool accessible and culturally appropriate?

- b. Work with ISD Director and DISO’s and/or Department Infrastructure team diligently to identify Gen AI before and throughout the procurement process. Many types of purchases may include elements of GenAI, even if the County is not intentionally seeking GenAI solutions. Staff must pay close attention to procurement involving deliverables in these areas, where GenAI is commonly generated:
 - i. Document drafting & summarization – automated generation of reports, contracts, or correspondence
 - ii. Customer service & communications – chatbots, virtual assistants, automated response systems
 - iii. Data analysis & forecasting – AI-driven insights, predictive modeling, trend analysis
 - iv. Training & education – AI-generated learning modules, simulations, instructional content
 - v. Creative content – automated design, video, or multimedia production
 - vi. Software development – code generation, testing automation, system documentation

- c. Identify the types of data any new AI technology will access and obtain written assurance from the AI vendor (i.e. through a Business Associate Agreement) that confidential data will be adequately protected against unauthorized access.

- d. Obtain written assurance from the AI vendor (i.e. through a Business Associate Agreement) that their systems can be configured to protect confidential data and comply with applicable data privacy laws and regulations.

- e. DISOs must complete a security and privacy assessment of third-party AI vendor to ensure their practices align with organizational policies. (see SJC-SEC-POL-16 “Vendor and Third-Party Management Policy” for further details)

- f. DISOs must conduct regular vulnerability assessments and security testing on AI tools and platforms to identify and address any security weaknesses or vulnerabilities. Modify\Prepare security assessments to include AI usage questions in the initial\annual vendor risk assessments reviews. (see SJC-SEC-POL-5 “RISK ASSESSMENT POLICY” for further details)

4. ASSET IDENTIFICATION

DISOs Shall:

- a. Identify and establish an inventory of all AI systems being used and/or maintained within a department and perform a risk assessment of the potential vulnerabilities and threats posed by those systems. Inventory must be continuously managed as and when new\existing AI systems are introduced and/or modified. Below information must be maintained as part of AI inventory:
 - a. System Name, Version and Vendor\Provider Name
 - b. Purpose and Use Case
 - c. Data Type (Types of data processed, generated, or accessed by the AI system (e.g., text, images, structured data).
 - d. Data Sources and Classification
 - e. Integrations\API interface

5. ACCESS AND SECURITY

County IT shall (or other staff as applicable):

- a. Restrict access to AI tools, platforms, or related systems used by County departments to authorized personnel only. Users must not share their access credentials or allow unauthorized individuals to use the AI tools on their behalf. (see SJC-SEC-POL-10 “ACCESS CONTROL POLICY”)
- b. Configure AI tools, platforms, or related systems securely, following industry best practices and vendor recommendations. This includes ensuring the configurations, latest updates, patches, and security fixes are applied in a timely manner. Few other key configuration practices are:
 - a. Use version control to track changes and maintain an audit trail.
 - b. Disable any unnecessary services, APIs, or ports on the AI platform to reduce the attack surface

- c. Implement strict validation on all inputs to prevent adversarial attacks, data injection, or other manipulative techniques.
 - d. Monitor and validate AI outputs to prevent data leakage or inadvertent disclosure of sensitive information.
- c. Implement strong authentication mechanisms, such as multi-factor authentication (MFA) for accessing AI tools and platforms. (see SJC-SEC-POL-16 “IDENTIFICATION AND AUTHENTICATION POLICY”)

6. DATA PROTECTION

County IT/DISOs shall:

- a. Develop firewall policies to restrict access to Open GenAI tools (e.g., OpenAI, ChatGPT, Grammarly, Gemini) unless the end user has requested and obtained an exception for a valid business use case. In case of exceptions, only county issued licensed version of Open Gen AI tool must be used.
- b. Implement Data Loss Prevention controls to prevent the input of confidential data into Open GenAI tools where such Open GenAI tools are required to support a valid business use case.
- c. Implement encryption and decryption of confidential data (e.g., ePHI) in accordance with county standards and applicable federal and state laws and regulations which govern the protection of such data. (see SJC-SEC-POL-8 “INFORMATION SYSTEM AND COMMUNICATIONS PROTECTION POLICY”)
- d. Implement Data Loss Protection controls to ensure compliance with data protection regulations and to secure confidential and regulated information, in environments where AI (Artificial Intelligence) systems are deployed.

7. MONITORING AND INCIDENT RESPONSE

County IT shall (or other staff as applicable):

- a. Implement appropriate logging and auditing mechanisms to capture activities related to AI system usage. These logs should be regularly reviewed to detect and respond to any suspicious or unauthorized activities (e.g. Record who accessed the AI system, what actions were taken and timestamps, configuration changes etc.)
- b. Report any suspected or confirmed security incidents related to AI system usage promptly to the organization's designated DISO. (see SJC-SEC-POL-17 “INCIDENT RESPONSE POLICY”)

8. TRAINING AND AWARENESS

Department Information Security Officers shall:

- a. Provide training to employees and relevant personnel on the responsible and secure use of AI. This training should cover topics such as ethical considerations, potential risks, security best practices, and compliance requirements.
- b. Conduct regular awareness campaigns and communications to reinforce the importance of cybersecurity, responsible AI usage, and adherence to this policy.
- c. Consider a phased approach to workforce training. Three recommended phases are organized by various disciplines to ensure training goals are met, resulting in effective leadership in using GenAI.
 - a. Phase 1: Executive Leadership, Legal, Labor and Privacy
 - b. Phase 2: Program Staff and Technical Experts
 - c. Phase 3: General Workforce
- d. Initial Training curriculum should include and appropriate curriculum to be assigned based on role.
 - a. General Education: Foundational introduction to AI, types of AI, potential business applications, potential risks, and comparing conventional AI versus GenAI.
 - b. Risk Intelligent GenAI Competencies: Introduction to GenAI, basic functional concepts, potential use cases and risk mitigation. Legal and privacy considerations of GenAI, data ownership, product ownership, and managing privacy risks.
- e. Technical Training: GenAI infrastructure, model management, model training, and output monitoring. Security considerations of GenAI, information security, and cybersecurity threat protection

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including termination, as well as potential civil and/or criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and any other actions deemed appropriate in County's sole discretion, as well as potential civil and/or criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO) and Chief Information Security Officer (CISO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, and actions and a timeframe for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests and confer with the requesting County Department.

DATE ISSUED/DATE REVIEWED

Date Issued:	04/14/2025
Date Reviewed:	03/11/2026

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53, NIST AI RMF (Artificial Intelligence Risk Management Framework) https://airc.nist.gov/AI_RMFKnowledgeBase/Playbook, Executive Order (EO) 13960 Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government, Executive Order N-12-23 by Governor Gavin Newsom to study the development, use, and risks of artificial intelligence

Policy #:	Title:	Effective Date:
SJC-SEC-POL-21	Information System and Communications Protection Policy	12/01/2023

PURPOSE

To establish guidelines for system and communications protection for County Information Technology (IT) resources and information systems.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. APPLICATION PARTITIONING

County IT shall:

- a. Separate user functionality from information system management functionality either logically or physically.

Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access.

2. INFORMATION IN SHARED RESOURCES

County IT shall:

- a. Prevent unauthorized and unintended information transfer via shared system resources.

This control prevents information, including encrypted representations of information, produced by the actions of prior users/roles from being available to any current users/roles (or current processes) that obtain access to shared system resources (e.g., registers, main memory, hard disks) after those resources have been released back to information systems.

3. DENIAL OF SERVICE PROTECTION

County IT shall:

- a. Ensure that the information system protects against or limit the effects of the denial-of-service attacks (not a comprehensive list): Ping sweep, port scanning etc by employing County defined security safeguards (as Imperva, network firewall, network segmentation, network zoning etc).

4. BOUNDARY PROTECTION

County IT shall:

- a. Monitor and control communications at the external boundary of the system and at key internal boundaries within the system.
- b. Implement sub-networks for publicly accessible system components that are separated from internal organizational networks and connected to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within security architecture.

5. TRANSMISSION CONFIDENTIALITY AND INTEGRITY

County IT shall:

- a. Deploy information systems that protect the confidentiality and integrity of transmitted information.

This control applies to both internal and external networks and all types of information system components from which information can be transmitted (e.g., servers, mobile devices, notebook computers, printers, copiers, scanners, facsimile machines).

- b. Implement technical security measures to guard against unauthorized access to confidential data (e.g., ePHI) that is being transmitted over county electronic communications networks.
- c. Implement technical security measures to ensure that electronically transmitted confidential data (e.g., ePHI) is not improperly modified without detection until disposed of.
- d. Where appropriate, implement a mechanism to encrypt confidential data (e.g., ePHI) in transit.

6. NETWORK DISCONNECT

County IT shall:

- a. Ensure information systems are configured to terminate the network connection associated with a communications session at the end of the session or after County defined time (as 3600 sec (TCP timeout)) of inactivity; this control applies to both internal and external networks.

Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection.

7. CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT

County IT shall:

- a. Establish and manage cryptographic keys for required cryptography employed within the information system in accordance with County standards for key generation, distribution, storage, access, and destruction.

8. CRYPTOGRAPHIC PROTECTION

County IT shall:

- a. Implement County standard cryptographic methods for appropriate use cases (e.g., use of TLS to secure website) in accordance with applicable federal and state laws, directives, policies, regulations, and standards.

Cryptography can be employed to support a variety of security solutions including, for example, the protection of classified and Controlled Unclassified Information, the provision of digital signatures, and the enforcement of information separation when authorized individuals have the necessary clearances for such information but lack the necessary formal access approvals.

- b. Implement encryption and decryption of confidential data (e.g., ePHI) in accordance with county standards and applicable federal and state laws and regulations which govern the protection of such data.

9. REMOTE ADMINISTRATION OF END USER DEVICES

County IT shall:

- a. Implement County standards to provide remote control (or administration) capabilities to County IT and third-party technical support personnel.
- b. Provide an explicit indication that remote administration \ control has been activated to users physically present at the devices.

10. PUBLIC KEY INFRASTRUCTURE CERTIFICATES

County IT shall:

- a. Issue public key certificates under a defined certificate policy or obtain public key certificates from an approved service provider (i.e. Digicert, Thawte, VeriSign etc).

- b. Manage information system trust stores for all key certificates to ensure only approved trust anchors are in the trust stores.

11. VOICE OVER INTERNET PROTOCOL

County IT shall:

- a. Establish usage restrictions and implementation guidance for Voice over Internet Protocol (VoIP) technologies as required by federal and state laws and regulations which govern the management of confidential data (e.g., ePHI).

12. SECURE NAME / ADDRESS RESOLUTION SERVICE

County IT shall:

- a. Utilize County standard methods and controls when implementing name \ address resolution services on County networks to prevent unauthorized modification of County namespaces and directories and to prevent the use of name resolution technologies to access and communicate with malicious or compromised Internet servers.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

DATE ISSUED/DATE REVIEWED

Date Issued:	04/15/2020
Date Reviewed:	03/11/2026

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP800-53a - System and Communications Protection (SC), NIST SP 800-12, NIST SP 800-28, NIST SP 800-41, NIST SP 800-52, NIST SP 800-56, NIST SP 800-57, NIST SP 800-58, NIST SP 800-77, NIST SP 800-81, NIST SP 800-95, NIST SP 800-100, NIST SP 800-111, NIST SP 800-113;

NIST Federal Information Processing Standards (FIPS) 140-2, FIPS 197, FIPS 199; State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.

HIPAA Security Rule: Encryption & Decryption: 45 CFR 164.312(a)(2)(iv)

HIPAA Security Rule: Transmission Security: 45 CFR 164.312(e)(1)

HIPAA Security Rule: Integrity Controls: 45 CFR 164.312(e)(2)(i)

HIPAA Security Rule: Encryption: 45 CFR 164.312(e)(2)(ii)

Policy #:	Title:	Effective Date:
SJC-SEC-POL-22	Information System Integrity Policy	12/01/2023

PURPOSE

To ensure that County Information Technology (IT) resources and information systems are established with system integrity monitoring to include areas of concern such as malware, application and source code flaws, industry supplied alerts and remediation of detected or disclosed integrity issues.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. FLAW REMEDIATION

County IT shall:

- a. Identify, report, and correct information system flaws.
- b. Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.
- c. Install security-relevant software and firmware updates for operating systems, applications, and infrastructure devices within 30 days of the release of the updates. If a patch or update cannot be applied, a compensating control must be applied (e.g. host firewall rule) to reduce the risk that a security vulnerability is exploited, and the compensating control must be documented.
- d. Incorporate flaw remediation into the County configuration management process.
- e. Employ automated mechanisms at least monthly to determine the state of information system components regarding flaw remediation.

2. MALICIOUS CODE PROTECTION

County IT shall:

- a. Employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.
- b. Update malicious code protection mechanisms whenever new releases are available in accordance with County configuration management policy and procedures.
- c. Configure malicious code protection mechanisms to:

- i. Perform periodic scans of the information system continuously and real-time scans of files from external sources at endpoint; network entry/exit points as the files are downloaded, opened, or executed in accordance with county security standards.
- ii. Block malicious code; quarantine malicious code; send alert to administrator; in response to malicious code detection.

3. INFORMATION SYSTEM MONITORING

County IT shall:

- a. Monitor the information system to detect:
 - i. Attacks and indicators of potential attacks.
 - ii. Unauthorized local, network, and remote connections.
- b. Identify unauthorized use of the information system through defined techniques and methods.
- c. Deploy monitoring devices strategically within the information system to collect system, user, place in network, etc. and at ad hoc locations within the system to track specific types of transactions of interest to the County.
- d. Protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
- e. Heighten the level of information system monitoring activity whenever there is an indication of increased risk to County operations and assets, individuals, other organizations, or based on law enforcement information, intelligence information, or other credible sources of information.
- f. Provide information system monitoring information to authorized personnel or business units as needed.

4. SYSTEM-GENERATED ALERTS

County IT shall ensure that:

- a. The information system that may be generated from a variety of sources, including, for example, audit records or inputs from malicious code protection mechanisms, intrusion detection or prevention mechanisms, or boundary protection devices such as firewalls, gateways, and routers will be disseminated to authorized personnel or business units that shall take appropriate action on the alert(s).

- b. Alerts be transmitted telephonically, electronic mail messages, or by text messaging as required. County personnel on the notification list can include system administrators, mission/business owners, system owners, or information system security officers.

5. SECURITY ALERTS, ADVISORIES, AND DIRECTIVES

County IT shall:

- a. Receive information system security alerts, advisories, and directives from external organizations (as vendors (PaloAlto, CrowdStrike, Tanium etc), California County Information Services Directors Association (CCISDA), Multi-State Information Sharing and Analysis Center (MS-ISAC), Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) etc) on an ongoing basis.
- b. Generate internal security alerts, advisories, and directives as deemed necessary throughout the County.
- c. Disseminate security alerts, advisories, and directives to: County defined personnel or roles (as Department Information Security Officers (DISOs), Chief Information Security Officer, other department personnel (i.e., department managers, directors), and County defined external organizations such as CCSIDA, MS-ISAC etc.
- d. Implement security directives in accordance with recommended time frames and threat severity.

6. SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY

County IT shall:

- a. Employ integrity verification tools to detect unauthorized changes to County defined software, firmware, and confidential data (e.g., ePHI);
- b. Incorporate the detection of unauthorized changes to the information system into the County incident response capability.

7. SPAM PROTECTION

County IT shall:

- a. Employ spam protection mechanisms at information system entry and exit points to detect and take action on unsolicited messages.
- b. Update spam protection mechanisms when new releases are available in accordance with County configuration management policy and procedures.

8. INFORMATION INPUT VALIDATION

County IT shall:

- a. Ensure the information system:
 - i. Checks the validity of information inputs and sanitization output.
 - ii. Provides a manual override capability for input validation.
 - iii. Restricts the use of the manual override capability to only County defined authorized individuals.
 - iv. Audits the use of the manual override capability.
 - v. Reviews and resolve within input validation errors.
 - vi. Behaves in a predictable and documented manner that reflects County and system objectives when invalid inputs are received.

9. INFORMATION INTEGRITY

County IT shall:

- a. Implement policies and procedures to protect confidential data (e.g., ePHI) from improper alteration or destruction. Implement electronic mechanisms to corroborate confidential data (e.g., ePHI) has not been altered or destroyed in an unauthorized manner.

10. ERROR HANDLING

County IT shall:

- a. Ensure the information system:
 - i. Generates error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries.
 - ii. Reveals error messages only to County defined personnel or roles.

11. INFORMATION HANDLING AND RETENTION

County IT shall:

- a. Handle and retain information within the information system and information output from the system in accordance with applicable state and federal laws, directives, policies, regulations, standards, and operational requirements.

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

DATE ISSUED/DATE REVIEWED

Date Issued:	04/15/2020
Date Reviewed:	03/11/2026

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – System and Information Integrity (SI), NIST SP 800-12, NIST SP 800-40, NIST SP 800-45, NIST SP 800-83, NIST SP 800-61, NIST SP 800-83, NIST SP 800-92, NIST SP 800-100, NIST SP 800-128, NIST SP 800-137, NIST SP 800-147, NIST SP 800-155;
State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.
HIPAA Security Rule: Integrity and Mechanism to Authenticate: 45 CFR 164.312(c)(1 and 2

Policy #:	Title:	Effective Date:
SJC-SEC-POL-23	Incident Response Policy	12/01/2023

PURPOSE

To ensure that county departments implement policies and procedures to address security incidents. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the department; and document security incidents and their outcomes.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. INCIDENT RESPONSE TRAINING

The County shall:

- a. Provide incident response training to information system users and system owners consistent with assigned roles and responsibilities; and
- b. Incorporate simulated events into incident response training to facilitate effective response by personnel in crisis situations.

2. INCIDENT HANDLING

The County shall:

- a. Implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; and
- b. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implement the resulting changes accordingly.

3. INCIDENT REPORTING

The County shall:

- a. Require personnel to report suspected security incidents to the department's Information Security Officer or Service Desk as soon as possible.
- b. Must develop and maintain a written process for users to report incidents. This process must include approved methods for reporting incidents including:

- a. Primary and secondary methods for reporting.
 - b. Specific recipients to receive incident reports
 - c. Any minimum information needed.
 - d. Timeframes for reporting incidents.
- c. The incident reporting process must be reviewed on an annual basis or following significant changes within the department.

4. INCIDENT RESPONSE PLAN

County IT shall:

- a. Develop an incident response plan that:
 - i. Identifies and responds to suspected or known security incidents;
 - ii. Mitigates to the extent practicable, harmful effects of security incidents that are known to the department.
 - iii. An incident manager and backup incident manager must be specifically identified by name within the plan
 - iv. Address any regulatory or other compliance requirements and communications
 - v. Documents security incidents and their outcomes.
- b. Update the incident response plan to address system/County changes or problems encountered during plan implementation, execution, or testing.
- c. The incident response process must be reviewed on an annual basis or following significant changes within the department. This review may also occur following an incident or tabletop exercise.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a timeframe for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests. confer with the requesting County Department.

DATE ISSUED/DATE REVIEWED

Date Issued:	04/15/2020
Date Reviewed:	03/11/2026

REFERENCE

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53a – Identification and Authentication (IA), NIST SP 800-12, NIST SP 800-63, NIST SP 800-73, NIST SP 800-76, NIST SP 800-78, NIST SP 800-100, NIST SP 800-116;
Homeland Security Presidential Directive (HSPD) 12 Policy for a Common Identification Standard for Federal Employees and Contractors;
Federal Information Processing Standards (FIPS): FIPS 201, FIPS 140;
State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.
HIPAA Security Rule: Security Incident Procedures: 45 CFR 164.308.(a)(6)(i and ii)

Policy #:	Title:	Effective Date:
SJC-SEC-POL-24	Cybercrime and Ransomware Incident Response Policy	07/01/2020

PURPOSE

To ensure that County Information Technology (IT) maintains technical and administrative controls to reduce the risk of a cybercrime or ransomware incident.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. TECHNICAL CONTROLS

County IT shall:

- a. Maintain technical controls to prevent or reduce the risk of a ransomware incident. County IT will review and observe best practices as recommended by the Cybersecurity Infrastructure and Security Agency; and
- b. Maintain encrypted, offline or immutable backups of information systems and data. See Countywide Information Security Policies - County Contingency Planning Policy - Information System Backup for further details.
- c. Maintain baselines or templates of critical information systems. See Countywide Information Security Policies – Configuration Management for further details.
- d. Perform periodic vulnerability scanning to identify and address vulnerabilities. Remediate critical and high vulnerabilities within one month of detection. See Countywide Information Security Policies – Risk Assessment Policy – Vulnerability Scanning for further details.
- e. Utilize multi-factor-authentication (MFA) for remote access sessions. See Countywide Information Security Policies – Access Control Policy – Remote Access for further details.
- f. Maintain malicious code protection mechanisms on endpoints and at information system entry and exit points. See Countywide Information Security Policies – County System and Information Integrity Policy – Malicious Code Protection for further details.
- g. Utilize the principle of least privilege to reduce the potential harm from a compromised user or device. See Countywide Information Security Policies –

Access Control Policy – Least Privilege for further details.

2. ADMINISTRATIVE CONTROLS

County IT shall (or other staff as applicable):

- a. Maintain administrative controls to reduce the risk and to limit the potential harm of a potential ransomware incident, including:
 - i. County Risk Management shall obtain and maintain Cyber Insurance that provides ransomware incident response services;
 - ii. Information Systems Division (ISD) shall maintain a Cybercrime and Ransomware Incident Response Procedure that describes the response, notification, coordination, and remediation steps to be followed during a ransomware incident;
 - iii. ISD shall maintain and deliver a Cybersecurity Awareness and Training Program in compliance with the County’s SECURITY AWARENESS AND TRAINING POLICY.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests. confer with the requesting County Department.

DATE ISSUED/DATE REVIEWED

Date Issued:	04/15/2020
Date Reviewed:	03/11/2026

REFERENCE

Cybersecurity and Infrastructure Security Agency: StopRansomware Guide:
<https://www.cisa.gov/stopransomware/ransomware-guide>

Policy #:	Title:	Effective Date:
SJC-SEC-POL-25	Contingency Planning Policy	12/01/2023

PURPOSE

To ensure that normal County Information Technology (IT) resources and information systems are available during times of disruption of services.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. CONTINGENCY PLAN

County IT shall (or other staff as applicable):

- b. Conduct a Business Impact Analysis (BIA) to define and develop the business continuity service level objectives that County IT must meet in the event of a disaster that disrupts information system operations or otherwise impacts the confidentiality, integrity, or availability of confidential data (e.g., ePHI). The BIA must:
 - i. Identify essential business functions and associated dependencies upon information systems and assets;
 - ii. Assess the relative criticality of specific applications and data in support of other contingency plan components;
 - iii. Define recovery objectives, restoration priorities, and metrics.

- c. Develop a Contingency Plan for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems identified in the BIA or which contain confidential data (e.g., ePHI). The contingency plan must:
 - i. Address contingency roles, responsibilities, and assigned individuals with contact information;
 - ii. Utilize data backups and duplicate copies of data as defined in the department's Data Back-up Plan;
 - iii. Govern the restoration of information systems as documented in the department's Disaster Recovery Plan;

- iv. Address maintaining essential missions and business functions despite an information system disruption, compromise, or failure as documented in the department's Emergency Mode Operation Plan.
 - v. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented.
- d. Maintain a Data Back-up Plan which describes how the department will create and maintain retrievable, exact copies of information assets including confidential data (e.g., ePHI) in accordance with County policies and standards. The Data Back-up Plan must address the following:
- i. The scope of information assets covered by the plan;
 - ii. A description of the back-up systems, media, and configuration supporting the plan, including the frequency, schedule and nature of back-ups;
 - iii. A procedure for retrieving data from back-ups in the event of a disaster.
- e. Develop a Disaster Recovery Plan which describes how the department will recover mission critical information systems and data assets including confidential data (e.g., ePHI) in the event of a disaster. The Disaster Recovery Plan must address the following:
- i. The scope of information systems protected by the plan;
 - ii. Procedures for recovering information systems and services utilizing the department's Disaster Recovery facilities;
 - iii. Procedures for obtaining access, if necessary, to the department's facilities in the event of a disaster in support of the restoration of lost data;
 - iv. Procedures for the eventual restoration of services in the department's primary data center facilities.
- f. Maintain an Emergency Mode Operation Plan which describes how the department will continue to provide its essential services in the event that its information systems become temporarily unavailable. The plan must address the following:
- i. The departmental services which are covered by the plan;
 - ii. The process for activating the plan and initiating Emergency Mode Operations;

- iii. Procedures for communicating with the department's workforce and its customers in the event that it initiates Emergency Mode Operations;
- iv. Procedures for providing essential services utilizing identified alternatives to its unavailable information systems and data assets; and
- v. For those departments that store or process confidential data such as electronic protected health information (ePHI), procedures for obtaining access to necessary confidential data (e.g., ePHI) during an emergency.

2. CONTINGENCY PLAN TESTING AND REVISION

County IT (or other staff as applicable):

- a. Periodically, but no less than annually, test and revise the Data Backup Plan, Disaster Recovery Plan, and Emergency Mode Operation Plan. The results of such testing must be reviewed and documented.

3. ALTERNATE STORAGE SITE

County IT shall (or other staff as applicable):

- a. Establish an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information. The alternate storage site must:
 - i. Provide information security safeguards equivalent to that of the primary site; and
 - ii. Be physically separated from the primary storage site to reduce susceptibility to the same threats.

4. ALTERNATE PROCESSING SITE

County IT shall (or other staff as applicable):

- a. Establish an alternate processing site including necessary agreements to permit the transfer and resumption of information system operations as outlined in the department's Contingency Plan. The alternate processing site must:
 - i. Provide information security safeguards equivalent to that of the primary site; and
 - ii. Be physically separated from the primary processing site to reduce susceptibility to the same threats.

5. INFORMATION SYSTEM BACKUP

County IT shall:

- a. Conduct backups of user-level and departmental information contained in the department's information systems as outlined in its Data Back-up Plan;
- b. Conduct backups of system-level information contained in the department's information systems as outlined in its Data Back-up Plan;
- c. Protect the confidentiality, integrity, and availability of backup information at storage locations; and
- d. Periodically test, but no less than annually, backup information to verify media reliability and information integrity.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County Information Technology (IT) resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting County Department.

DATE ISSUED/DATE REVIEWED

Date Issued:	04/15/2020
Date Reviewed:	03/11/2026

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP):
NIST SP 800-53a – Contingency Planning (CP), NIST SP 800-16, NIST SP 800-34, NIST SP 800-50, NIST SP 800-84;
NIST Federal Information Processing Standards (FIPS) 199;
State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.

HIPAA Security Rule: Contingency Plan: 45 CFR 164.308.(a)(7)(i)
HIPAA Security Rule: Data Back-up Plan: 45 CFR 164.308.(a)(7)(ii)(A)
HIPAA Security Rule: Disaster Recovery Plan: 45 CFR 164.308.(a)(7)(ii)(B)
HIPAA Security Rule: Emergency Mode Operation Plan: 45 CFR 164.308.(a)(7)(ii)(C)
HIPAA Security Rule: Testing and Revision Procedures: 45 CFR 164.308.(a)(7)(ii)(D)
HIPAA Security Rule: Application and Data Criticality Analysis: 45 CFR 164.308.(a)(7)(ii)(E)
HIPAA Security Rule: Emergency Access Procedure: 45 CFR 164.312.(a)(2)(ii)

Policy #:	Title:	Effective Date:
SJC-SEC-POL-26	Data Classification Policy	12/01/2023

PURPOSE

To ensure that County Information Technology (IT) and County Data Owners properly classify and protect data that is created, stored, processed, or transmitted within County Departments.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. DATA CLASSIFICATION

County IT shall (or other staff as applicable):

- a. Classify all data created, stored, processed, or transmitted on department information systems according to the impact to the county or residents resulting from the disclosure, modification, breach or destruction of the data, or as required by applicable federal and state law and regulation;
- b. Classify data as Confidential if it falls under one or more of the following categories:
 - i. Data that is protected from unauthorized disclosure based on federal or state laws, regulations, or other legal agreements;
 - ii. Protected Health Information;
 - iii. Financial Account Data;
 - iv. Payment Card Data;
 - v. Criminal Justice Records and Information;
 - vi. Personal Identifying Information (except as determined to be public record);
 - vii. Federal Tax Information;
 - viii. Other protected data as designated by a Department Director.
- c. Classify all data that is not confidential as Public.

2. DATA MANAGEMENT

County IT shall (or other staff as applicable):

- a. Maintain an asset inventory of all Confidential data, including information about the nature of the data, and the information systems, hardware assets, or external information services that store or process the confidential data;
- b. Label assets and configuration items containing Confidential data in a Configuration Management Database per County standards; and
- c. Assign a Data Owner to all significant stores of Confidential data. Unless otherwise specified, the Department Director of the department creating or holding the confidential data is to be assigned as the Data Owner.

3. DATA HANDLING

County IT shall (or other staff as applicable):

- a. Restrict and enforce access to Confidential data to workforce members who have authorized access and need such access to perform their duties, or as otherwise designated by the Data Owner;
- b. Protect Confidential data per applicable federal and state laws and regulations and County Policies;
- c. Report mis-disclosures of Confidential data to the Data Owner and per applicable federal and state laws and regulations and County Policies.

4. DATA ENCRYPTION

County IT shall (or other staff as applicable):

- a. Encrypt Confidential data stored at rest per County Standards;
- b. Encrypt Confidential data transmitted externally per County Standards.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests. confer with the requesting County Department.

DATE ISSUED/DATE REVIEWED

Date Issued:	12/01/2023
Date Reviewed:	03/11/2026

REFERENCE

Policy #:	Title:	Effective Date:
SJC-SEC-POL-27	Security Management Policy	07/01/2020

PURPOSE

To ensure that County Departments assign resources and implement departmental policies and procedures to enforce the Countywide Information Security Policies, and to prevent, detect, contain, and correct security violations.

POLICY

This policy is applicable to all County departments and users of County resources and assets.

1. SECURITY ROLES AND RESPONSIBILITIES

- a. The Information Systems Division (ISD) Director shall designate a Chief Information Security Officer (CISO) who is responsible for overseeing and monitoring the cybersecurity programs and activities of all County departments. The CISO will annually report to the Board of Supervisors (BOS) and the County Administrator’s Office (CAO) on the state of the County’s cybersecurity program(s), risks to the confidentiality, integrity, and availability of County information assets, and risks of non-compliance with federal and state laws and regulations which govern confidential data (e.g., electronic protected health information (ePHI)).
 - i. As of 09/09/2024, Amanpreet Kaur is assigned CISO for the County.
- b. Department Directors shall designate Department Information Security Officers (DISOs) who are responsible for directing and implementing cybersecurity programs, activities, and controls within their respective departments in compliance with County policies and standards and federal and state laws and regulations which govern confidential data.
 - i. DISOs must hold an Information Systems Analyst (ISA) or Departmental Information Systems Analyst (DISA) classification, must have skills and experience in information security, and must have sufficient organizational seniority to ensure that the Countywide Information Security Policies are enforced within the Department.
 - ii. Once designated, the Director must update departmental policies and procedures to identify the designated DISO and inform departmental staff and must notify the CISO of the designation. The CISO has the authority to approve or reject DISO assignments made by Department Directors.

- c. Department Directors who oversee regulated data (e.g., ePHI as regulated by HIPAA) shall designate Information Security Officers (ISOs) who are responsible for the Department's compliance with the relevant laws and regulations. ISD recommends that Department Directors assign the same person the role of DISO and ISO. Directors may, however, assign a staff member with unique knowledge or experience with the relevant laws and regulations to fill the role.
- d. The CISO shall organize a Countywide Information Security Steering Committee (CISSC) to coordinate information security activities among County Departments. Membership on the CISSC shall include the CISO, the ISD Director, the Assistant ISD Directors and all DISOs. Meetings will be held at least bi-annually.

2. RISK ANALYSIS

- a. Department Information Security Officers shall conduct a thorough analysis of all information networks and systems containing confidential data (e.g., ePHI) on a periodic, ongoing basis, to document the threats and vulnerabilities to stored and transmitted information. See SECURITY ASSESSMENT POLICY.

3. RISK MANAGEMENT

- a. County IT shall implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. See RISK MANAGEMENT POLICY.

4. INFORMATION SECURITY AUDITS

- a. The CISO shall periodically conduct audits of county departments to assess their compliance with the Countywide Information Security Policies and to evaluate the robustness of their Information Security programs. The results of these audits will be included in the CISO's annual report to the CAO and the Board.
- b. DISOs are required to respond timely and completely to all audit requests made by the CISO.

5. SANCTION POLICY

- a. Department Directors and County Human Resources will apply appropriate sanctions against workforce members who fail to comply with these Countywide Information Security Policies and procedures. See PERSONNEL SECURITY POLICY.

6. INFORMATION SECURITY ACTIVITY REVIEW

- a. DISOs shall implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. See AUDITING AND ACCOUNTABILITY POLICY.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the County Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests. confer with the requested County Department.

DATE ISSUED/DATE REVIEWED

Date Issued:	12/1/2023
Date Reviewed:	03/11/2026

Policy #:	Title:	Effective Date:
SJC-SEC-POL-28	Internet of Things (IoT) and Operational Technology (OT) Devices Policy	04/14/2025

PURPOSE

As the adoption of IoT and OT devices continues to grow, it is essential to ensure that these devices are deployed, managed and monitored in order in a method that protects confidential data and enhancing the County’s overall cybersecurity posture.

The purpose of this policy is to establish guidelines for the secure configuration and responsible use of Internet of Things (IoT) and Operational Technology (OT) devices within the County to ensure data integrity, privacy, and compliance with applicable laws and regulations.

DEFINITIONS

Internet of Things (IoT): A network of interconnected devices that communicate and exchange data with one another.

IoT Device(s): Any physical device that connects to the internet and can collect, send or receive data (e.g., sensors, security cameras, smart appliances, smartwatches, patient monitoring devices, fitness trackers) without requiring human-to-human or human-to-computer interaction.

Operational Technology (OT) Device(s): refer to hardware and software that detect or control physical equipment, processes that provide critical services including but not limited to Water and Waste Management (SCADA Systems), Emergency Dispatch systems, HVAC control systems, Access Control systems, Traffic Signal Control Systems.

Workforce: For this policy workforce is defined as employees, members of professional staff, affiliates and contracted individuals and vendors of San Joaquin County

POLICY

This policy applies to all departments, employees, contractors, and third-party service providers that deploy or manage IoT and OT devices within the County’s network infrastructure.

- 8. IDENTIFICATION
County ITAgencies shall:

- a. All departments must obtain approval from County\Agency IT department for connection of IoT and OT device(s) to County's network by sending an email or Submitting ticket to County\Agency IT Service Desk Team. Request must include details but not limited to
 - a. Device Name, Type, Manufacturer and Model number
 - b. Device Purpose and Functionality
 - c. Connection type (Analog, Wired\Ethernet or Wi-Fi\ Wireless)
 - d. Network IP Address requirement (Dynamic or Static)
 - e. Network Port and VLAN
- b. Must establish procedure to identify and register all IoT and OT devices connecting to County's network and maintain inventory.
- c. All IoT and OT devices connecting to County network are subject to audit as part of County's continuous monitoring process.
- d. IoT and OT Device not managed by County can only be allowed access to Guest wireless network.

9. DEVICE SECURITY, ACCESS CONTROL AND DATA PROTECTION
County IT\Agencies shall:

- a. Configure strong unique passwords and change default credentials for IoT Devices. See SJC-SEC-POL-10 Access Control Policy in County Information Security Policy for further guidelines on establishing secure access.
- b. Must configure network segmentation following below requirements:
 - i. IoT and OT Devices must be connected to separate VLAN from non-IoT\OT devices (e.g. Desktops, Phones, Printers, Servers etc.) to limit exposure to internal systems.
 - ii. Network VLANs designated for IoT and OT devices must be segmented from the rest of the organizational network to minimize exposure to potential threats by using segmentation firewall and/or data center firewalls.
 - iii. Firewall policies must be configured to enforce the restricted access between Non-IoT\OT and IoT\OT Device network (e.g. Define allowed ports/Ip address/protocols only)
- c. Must establish a procedure for assessing and deploying firmware and software updates to address security vulnerabilities.

- d. Establish an encrypted transmission channel utilizing an encryption protocol, such as TLS or SSL. For TLS, County IT must ensure that IoT and OT devices are configured to use the latest approved version of the encryption protocol, provided the device supports it. If the device does not support the latest version, prepare remediation plan including mitigation strategy to segment/isolate the device and \or explore alternative options for encryption and\or device update\replacement plan. (see See SJC-SEC-POL-5 “Risk Assessment Policy) in County Information Security Policy for further guidelines).
- e. Protected and confidential data collected from IoT and OT devices must be encrypted both at rest and in transit.
- f. Implement data retention policies in accordance with applicable state and federal laws, directives, policies, regulations, standards, and operational requirements. Critical data from IoT devices must be backed up regularly and ensure that backups are stored securely. See SJC-SEC-POL-15 Contingency Planning Policy in County Information Security Policy for further guidelines.

10. DEVICE AUDITING, MONITORING AND LOGGING:

County IT\Agencies shall:

- a. DISO (Designated Information Security Officer) must perform regular vulnerability scans of all IoT and OT Devices by following County Information Security Policy SJC-SEC-POL-5 RISK ASSESSMENT POLICY.
- b. IoT and OT networks and devices must be monitored to detect abnormal traffic and emerging threats, as well as to track device performance logs. These logs and events should be directed to a designated logging system, where they will be assigned a severity level and regularly reviewed for signs of unauthorized access or anomalies. Additionally, these logs must be retained in audit log records.
- c. County IT\Agencies must have Incident Response Plan prepared and\or updated to include IoT and OT device specific security incident.

COMPLIANCE

Any violation of this policy may result in discipline up to and including termination of employment, and/or may result in suspension from County systems.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a timeframe for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

DATE ISSUED/DATE REVIEWED

Date Issued:	04/14/2025
Date Reviewed:	03/11/2026

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53 – Personal Owned Device (SR), NIST CSF 2.0 GOVERN(GV).OV-01, ISO/IEC 27001:2022, NIST SP 800-63, NIST SP 800-66, HIPAA Security Rule; Federal Information Processing Standards (FIPS) 140-2, FIPS 197, FIPS 201.

Policy #:	Title:	Effective Date:
SJC-SEC-POL-29	Cloud Services Security Policy	03/11/2026

PURPOSE

The purpose of this policy is to establish processes and procedures for cloud service providers, their responsibilities, and management strategies to ensure the confidentiality, integrity, and availability of County applications and data. It applies to all county departments, entities employees, contractors, and authorized users who access, use, or manage cloud services on behalf of their organization.

DEFINITIONS

Cloud computing: Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud computing promotes availability and is composed of five essential characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.

Cloud computing deployment models: Cloud technologies can be deployed as private, community, public, or hybrid clouds.

Cloud Service Provider (CSP): A company that offers some component of cloud computing — typically Infrastructure as a Service (IaaS), Software as a Service (SaaS) or Platform as a Service (PaaS) to other businesses or individuals.

Workforce: For this policy workforce is defined as employees, members of professional staff, affiliates and contracted individuals and vendors of San Joaquin County

POLICY

Cloud technology has expanded and allows almost any IT related resource to be offered as a service. Taking advantage of these benefits requires that appropriate controls and risks are managed related to the County assets, data, and property. This policy is applicable to all departments and users of County resources and assets.

- b. CLOUD SERVICE PROVIDER(CSP) SELECTION PRELIMINARY REQUIREMENT
County Department\IT Shall

- a. Cloud providers must be able to comply with requirements as established within the relevant County Information Security Policies, including this document.
- b. Formal security review of the cloud service must be conducted prior to the procurement of the service and written approval by County IT Security
- c. Agencies must anticipate and mitigate risks where possible of cloud-hosted data and resources in accordance with the San Joaquin County Information Security Policy

c. VENDOR ASSESSMENT

County Department\IT Shall

- a. DISOs must complete a security and privacy assessment of CSP to ensure their practices align with organizational policies. (see SJC-SEC-POL-16 “Vendor and Third-Party Management Policy” for further details)
- b. DISOs must conduct regular vulnerability assessments and security testing on cloud solutions to identify and address any security weaknesses or vulnerabilities. Modify\Prepare security assessments to include cloud solutions questions in the initial\annual vendor risk assessments reviews. (see SJC-SEC-POL-5 “RISK ASSESSMENT POLICY” for further details)
- c. Any violation of security measures affecting the security of County information or resources that is discovered by County IT must be communicated with the CSP as soon as possible after discovery so the CSP can address the concern.

d. PRIVACY AND SECURITY CONTROLS FOR CLOUD HOSTING

County IT Shall (or other staff as applicable)

- a. Ensure that cloud provider’s electronic discovery capabilities, processes, and policies do not compromise the privacy and security of County sensitive data hosted by the CSP and obtain written assurance from the CSP (i.e. through a Business Associate Agreement) that confidential data will be adequately protected against unauthorized access.
- b. Where possible, ensure hosted systems or services will allow County IT to monitor the services for up-time, availability and security functionality. Maintain logs of user access and system events; integrate with County monitoring tools where feasible. Vulnerability assessments and audits must be conducted periodically.
- c. Understand applicable underlying technologies that the cloud providers use to host services and how that integrates with current County on premise infrastructure if such integration exists.

- d. Ensure relevant safeguards are in place to secure authentication, authorization, and other identity and access-management functions in accordance with the requirements outlined in the County Access Control Policy and Identification and Authentication Policy.
- e. Encrypt data at rest and in transit; sensitive data must always be encrypted in accordance with the Information System and Communications Protection Policy
- f. CSPs should certify that in multi-tenant offerings the structure or architecture of their systems are capable of isolating hosted data and operations from other tenants where possible.
- g. Establish an SLA with the CSP for notification of service disruption as well as resuming critical operations within an agreed upon time.
- h. Ensure that the cloud provider promptly notifies the County of any security incidents; the County will follow its incident response procedures.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

DATE ISSUED/DATE REVIEWED

Date Issued:	03/11/2026
--------------	------------

Date Reviewed: 03/11/2026

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-144 – Security and Privacy in Public Cloud Computing, NIST SP 800-145 – The NIST Definition of Cloud Computing; NIST SP 500-292 – Cloud Computing Reference Architecture; Federal Information Processing Standards (FIPS) 140-3, FIPS 199, FIPS 200; HIPAA Security Rule – 45 CFR §164.302–318

Policy #:	Title:	Effective Date:
SJC-SEC-POL-30	Encryption Key and Certificate Management Policy	03/11/2026

PURPOSE

The purpose of this policy is to establish requirements for selecting cryptographic keys, managing keys, assigning key strength and using and managing digital certificates. Encryption can be an effective protection control when it is necessary to possess County Information confidential. Encryption is not a substitute for other information protection controls, such as access control, authentication or authorization. County Information Encryption must be used in conjunction with other controls.

DEFINITIONS

Algorithm – A procedure or formula for solving a problem

Asymmetric-key algorithm – http://en.wikipedia.org/wiki/Public_key_cryptography

Cipher – A cipher is any method of encrypting text (concealing its readability and meaning). It is also sometimes used to refer to the encrypted text message itself although here the term ciphertext is preferred.

Ciphertext - Ciphertext is encrypted text. Plaintext is what you have before encryption, and ciphertext is the encrypted result. The term cipher is sometimes used as a synonym for ciphertext, but it more properly means the method of encryption rather than the result.

Cryptoperiod - A cryptoperiod is a specific time span during which a cryptographic key setting remains in effect. A key uses an algorithm to create ciphertext from plaintext and, for the receiver of the encrypted text, to decipher it. Once the cryptoperiod ends, the key is no longer available for either encryption or decryption.

Decryption - the process of converting encrypted data back into its original form, so it can be understood.

Encryption - The conversion of data into a form, called a ciphertext, that cannot be easily understood by unauthorized people.

Key – In cryptography, a key is a variable value that is applied using an algorithm to a string or block of unencrypted text to produce encrypted text, or to decrypt encrypted text. The length of the key is a factor in considering how difficult it will be to decrypt the text in a given message.

Plaintext - Ordinary readable text before being encrypted into ciphertext or after being decrypted.

Encryption- is used to refer to both the process of encrypting and the process of decrypting information. The term encryption key therefore refers to the keys needed for encryption and those needed for decryption.

POLICY

This policy is applicable to all departments and users of County resources and assets. The County IT must use industry-approved strong algorithms.

9. PROTECTING KEYS

The County IT must protect private encryption keys to prevent their unauthorized disclosure and subsequent fraudulent use. The keys used to encrypt data should not be stored on the same media as that data. Whenever keys are stored either physically or logically in close proximity to the data that it is protecting, mitigating controls must be in place to ensure a compromise of the data does not happen. Such mitigating controls must include, but are not limited to, the encryption of the keys themselves

10. PRIVATE KEY HANDLING

The County IT Shall

- a. County IT Department handling private keys must:
 - a. Must Physically and logically secure them.
 - b. Store keys in/on:
 - i. An encrypted key store or in an otherwise encrypted form.
 - ii. A security token.
 - iii. An Encryption keyring.
 - c. Not share the key with anyone other than those authorized.
 - d. Never store the key(s) on the same IT Resource as the County Information being protected at rest (e.g., encrypted storage).
 - e. Never reuse the key(s) to encrypt another set of unrelated or separate County Information.

11. GENERATING STRONG KEYS

The County IT personnel generating private keys must:

- a. Select a key size using the minimum specified by the encryption method or greater when symmetric key encryption is employed.
- b. Generate keys on the IT Resource itself or, if transmission of a private key is required, distribute keys manually using a public key transport mechanism or using a previously distributed or agreed-upon key encrypting key.
- i. Use a random key generation mechanism or Keys must be generated by cryptographic algorithms approved by County IT Department

12. ACCESS TO KEYS

The County IT

- a. Must provide access to private keys limited to those who have a need-to-know based on job responsibilities.
- b. Must have auditable procedures in place to provide access to private keys in the event of an emergency and/or the passphrase holder being unavailable.

13. CHANGING PRIVATE KEYS AND THE PRIVATE KEY LIFECYCLE

The County IT must:

- a. Have a process to approve key changes, record dispositions and change keys when a Workforce Member with access to a private key(s) separates or changes roles.
- b. Have a process to change keys as part of the response to an Information Security Incident at least once annually.
- c. Private keys must be revoked and/or deleted when they are no longer needed to perform a business function.
- d. Private keys must not be re-issued or reused.

14. ENCRYPTION KEY BACKUP AND DR TESTING

The County IT shall

- a. Perform routine annual testing of key recovery and should be based on the DR/BC plan associated with the system.
- b. Must backup the private key associated with any encryption at rest of County Information.

15. ENCRYPTION METHOD

The County IT must select the stronger of the following methods:

- a. An encryption method based on the Risk Assessment.
- b. Symmetric - using the minimum recommended key strength or higher; or
- c. Asymmetric/Public-Private key pair - using the minimum recommended key strength or higher.

16. COMPROMISED KEYS

The County IT must

- a. Change encryption keys immediately if the key becomes compromised or is discovered by any unauthorized person or party
- b. Report any compromised key to the County Information Security team

17. WEB SERVER CERTIFICATES

The County IT shall

- a. Use digital certificates signed by an IT-approved certificate authority (CA).
- b. Select a key size of 2048 bits or greater.
- c. Select an expiration of not more than one (1) year
- d. Use a new public-private key pair when the certificate is renewed. (The public key is sent as part of the CSR - Certificate Signing Request.)
- e. Not use wildcard digital certificates for top level domains or subdomains accessing County sensitive data

18. SELF-SIGNED CERTIFICATES

The County IT must

- a. Not use them for any production purpose on a public network
- b. Not use them for the testing of IT Resources processing, storing or transmitting sensitive and/or confidential data
- c. IT assets with factory-installed self-signed certificates can only be used on protected private networks.

19. LOGGING AND AUDIT

The County IT shall

- a. Ensure all encryption key activities - including creation, access, use, rotation, and deletion are securely logged and routinely audited to maintain integrity, accountability, and compliance
- b. Ensure all certificate issuance, renewal, revocation, and usage events are centrally logged and routinely audited to maintain integrity, trust, and compliance.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a time-frame for achieving the minimum compliance level with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

DATE ISSUED/DATE REVIEWED

Date Issued:	03/11/2026
Date Reviewed:	03/11/2026

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-130, A Framework for Designing Cryptographic Key Management Systems NIST CSF 2.0 GOVERN(GV).OV-01, ISO/IEC 27001:2022, NIST SP 800-57 Part 1 Rev. 5 Recommendation for Key Management: Part 1 – General, OWASP Key Management Cheat Sheet ; ISO 27002:2022 requirements are met by this Standard

Policy #:	Title:	Effective Date:
SJC-SEC-POL-31	Zero Trust Architecture Policy	03/11/2026

PURPOSE

The purpose of this policy is to define the Zero Trust Architecture (ZTA) requirements that San Joaquin County should adopt to improve security posture, reduce risk, and ensure continuous verification of access to County resources. Zero Trust assumes that no user, device, or network segment is implicitly trusted, regardless of location.

DEFINITIONS

Zero Trust: means never assuming anyone is safe and always double-checking every user and device before letting them access anything. A cybersecurity approach that requires continuous verification of identity and trust for all access.

Zero Trust Architecture (ZTA): means never trusting any user or device by default and always verifying identity, access, and security before allowing anything to connect or interact.

Micro-Segmentation: Dividing network resources into granular segments to reduce risk.

Lateral Movement: When hackers move across systems or computers in a network to access more information than they initially could.

Identity-based: Access or actions in a system that are controlled and tracked based on who the user is, rather than just the device or network location.

POLICY

This policy is applicable to all departments and users of County resources and assets. San Joaquin County shall adopt a Zero Trust Architecture core principle Never Trust, Always Verify, Least Privilege Access and Micro-Segmentation. This will help eliminate implicit trust and require verification of identity, device health, authorization, and risk level for every access request.

20. ZERO TRUST ARCHITECTURE REQUIREMENTS

County IT must (or other staff as applicable):

h. DEVICE TRUST:

- i. All users, devices, applications, and services must be continuously authenticated and authorized before accessing County resources. Access

- decisions must leverage contextual information including identity, device health, location, and risk level.
- ii. Validate end user device posture (For e.g. patching status, configuration compliance, malware protection) before granting access to County systems and ensure that only managed and/or compliant devices may access County resources.
- i. **ACCESS CONTROL: Refer to **SJC-SEC-POL-1 Access Control Policy for additional guidance****
 - i. Ensure that all users are authenticated using Multi-Factor Authentication (MFA).
 - ii. Privileged access accounts must be regularly reviewed, monitored, and logged and Temporary\Emergency access must be controlled and revoked after use.
 - iii. Access must be limited to minimum necessary to perform assigned tasks and access should be evaluated on an annual basis and/or if there are major changes.
 - j. Configure firewall rules\policies to deny-by-default. Networks and systems must be segmented into isolated zones to limit lateral movement and contain potential threats. County IT must implement monitoring and logging to detect suspicious activity between isolated zones\segments.
 - k. Ensure remote access is using encrypted, identity-based access methods and comply with multi-factor authentication (MFA). All connections from untrusted networks or devices must be verified before access is granted to County systems.
 - l. All access, authentication, and network activity must be logged, monitored, and analyzed to detect anomalous or malicious behavior. Security alerts must be promptly investigated and remediated. Refer to **SJC-SEC-POL-23 Incident Response Policy for additional guidance**.

COMPLIANCE

County employees who violate this policy may be subject to appropriate disciplinary action up to and including discharge as well as both civil and criminal penalties. Non-County employees, including, without limitation, contractors, may be subject to termination of contractual agreements, denial of access to County IT resources, and other actions as well as both civil and criminal penalties.

POLICY EXCEPTIONS

Requests for exceptions to this policy shall be reviewed by the Chief Information Security Officer (CISO) and the Chief Information Officer (CIO). Departments requesting exceptions shall provide such requests to the CIO. The request should specifically state the scope of the exception along with justification for granting the exception, the potential impact or risk attendant upon granting the exception, risk mitigation measures to be undertaken by the IT Department, initiatives, actions and a timeframe for achieving the minimum compliance level

with the policies set forth herein. The CIO shall review such requests; confer with the requesting department.

DATE ISSUED/DATE REVIEWED

Date Issued:	03/11/2026
Date Reviewed:	03/11/2026

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP NIST SP 800-207, "Zero Trust Architecture", CISA Zero Trust Maturity Model Guidance, NIST SP 800-53, Security and Privacy Controls, NIST ZTA Planning Guide.

Appendix A: Glossary

Business Owner (BO) is department head or their designed individuals

Department Information Security Officer(s) (DISOs) are security person from each department

Security team consists of Chief Information Security Officer and Department Information Security Officer(s)

COMMON TERMS AND DEFINITIONS

Appendix A provides definitions for security terminology used within Special Publication 800-53. Unless specifically defined in this glossary, all terms used in this publication are consistent with the definitions contained in CNSS Instruction 4009, *National Information Assurance Glossary*.

Adequate Security [OMB Circular A-130, Appendix III, Adapted]	Security commensurate with the risk resulting from the loss, misuse, or unauthorized access to or modification of information.
Advanced Persistent Threat	An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives.
Agency	See <i>Executive Agency</i> .
All Source Intelligence [Department of Defense, Joint Publication 1-02]	Intelligence products and/or organizations and activities that incorporate all sources of information, most frequently including human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open-source data in the production of finished intelligence.
Assessment	See <i>Security Control Assessment</i> .
Assessor	See <i>Security Control Assessor</i> .
Assurance [CNSSI 4009]	Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy.

Assurance Case [Software Engineering Institute, Carnegie Mellon University]	A structured set of arguments and a body of evidence showing that an information system satisfies specific claims with respect to a given quality attribute.
Audit Log [CNSSI 4009]	A chronological record of information system activities, including records of system accesses and operations performed in a given period.
Audit Record	An individual entry in an audit log related to an audited event.
Audit Reduction Tools [CNSSI 4009]	Preprocessors designed to reduce the volume of audit records to facilitate manual review. Before a security review, these tools can remove many audit records known to have little security significance. These tools generally remove records generated by specified classes of events, such as records generated by nightly backups.
Audit Trail [CNSSI 4009]	A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security-relevant transaction from inception to final result.
Authentication [FIPS 200]	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
Authenticator	The means used to confirm the identity of a user, processor, or device (e.g., user password or token).
Authenticity	The property of being genuine and being able to be verified and trusted; confidence in the validity of a transmission, a message, or message originator. See <i>Authentication</i> .
Authorization (to operate)	The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.
Authorization Boundary	All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.
Authorize Processing	See <i>Authorization</i> .
Authorizing Official	A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Availability [44 U.S.C., Sec. 3542]	Ensuring timely and reliable access to and use of information.
Baseline Configuration	A documented set of specifications for an information system, or a configuration item within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures.
Blacklisting	The process used to identify: (i) software programs that are not authorized to execute on an information system; or (ii) prohibited Universal Resource Locators (URL)/websites.
Boundary Protection	Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communications, through the use of boundary protection devices (e.g., gateways, routers, firewalls, guards, encrypted tunnels).
Boundary Protection Device	A device with appropriate mechanisms that: (i) facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or (ii) provides information system boundary protection.
Central Management	The organization-wide management and implementation of selected security controls and related processes. Central management includes planning, implementing, assessing, authorizing, and monitoring the organization-defined, centrally managed security controls and processes.
Chief Information Officer [PL 104-106, Sec. 5125(b)]	<p>Agency official responsible for:</p> <ul style="list-style-type: none"> (i) Providing advice and other assistance to the head of the executive agency and other senior management personnel of the agency to ensure that information technology is acquired and information resources are managed in a manner that is consistent with laws, Executive Orders, directives, policies, regulations, and priorities established by the head of the agency; (ii) Developing, maintaining, and facilitating the implementation of a sound and integrated information technology architecture for the agency; and (iii) Promoting the effective and efficient design and operation of all major information resources management processes for the agency, including improvements to work processes of the agency. <p>Note: Organizations subordinate to federal agencies may use the term <i>Chief Information Officer</i> to denote individuals filling positions with similar security responsibilities to agency-level Chief Information Officers.</p>
Chief Information Security Officer	See <i>Senior Agency Information Security Officer</i> .

Chief Privacy Officer	See <i>Senior Agency Official for Privacy</i> .
Classified Information	Information that has been determined: (i) pursuant to Executive Order 12958 as amended by Executive Order 13526, or any predecessor Order, to be classified national security information; or (ii) pursuant to the Atomic Energy Act of 1954, as amended, to be Restricted Data (RD).
Commodity Service	An information system service (e.g., telecommunications service) provided by a commercial service provider typically to a large and diverse set of consumers. The organization acquiring and/or receiving the commodity service possesses limited visibility into the management structure and operations of the provider, and while the organization may be able to negotiate service-level agreements, the organization is typically not in a position to require that the provider implement specific security controls.
Common Carrier	In a telecommunications context, a telecommunications company that holds itself out to the public for hire to provide communications transmission services. Note: In the United States, such companies are usually subject to regulation by federal and state regulatory commissions.
Common Control [NIST SP 800-37; CNSSI 4009]	A security control that is inheritable by one or more organizational information systems. See <i>Security Control Inheritance</i> .
Common Control Provider [NIST SP 800-37]	An organizational official responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inheritable by information systems).
Common Criteria [CNSSI 4009]	Governing document that provides a comprehensive, rigorous method for specifying security function and assurance requirements for products and systems.
Common Secure Configuration	A recognized standardized and established benchmark that stipulates specific secure configuration settings for a given information technology platform.
Compensating Security Controls [CNSSI 4009, Adapted]	The security controls employed in lieu of the recommended controls in the security control baselines described in NIST Special Publication 800-53 and CNSS Instruction 1253 that provide equivalent or comparable protection for an information system or organization.

Computer Matching Agreement	An agreement entered into by an organization in connection with a computer matching program to which the organization is a party, as required by the Computer Matching and Privacy Protection Act of 1988. With certain exceptions, a computer matching program is any computerized comparison of two or more automated systems of records or a system of records with nonfederal records for the purpose of establishing or verifying the eligibility of, or continuing compliance with, statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to cash or in-kind assistance or payments under federal benefit programs or computerized comparisons of two or more automated federal personnel or payroll systems of records or a system of federal personnel or payroll records with non-federal records.
Confidentiality [44 U.S.C., Sec. 3542]	Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.
Configuration Control [CNSSI 4009]	Process for controlling modifications to hardware, firmware, software, and documentation to protect the information system against improper modifications before, during, and after system implementation.
Configuration Item	An aggregation of information system components that is designated for configuration management and treated as a single entity in the configuration management process.
Configuration Management	A collection of activities focused on establishing and maintaining the integrity of information technology products and information systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.
Configuration Settings	The set of parameters that can be changed in hardware, software, or firmware that affect the security posture and/or functionality of the information system.
Controlled Area	Any area or space for which an organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and/or information system.
Controlled Interface [CNSSI 4009]	A boundary with a set of mechanisms that enforces the security policies and controls the flow of information between interconnected information systems.

Controlled Unclassified Information [E.O. 13556]	A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the federal government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.
Countermeasures [CNSSI 4009]	Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of an information system. Synonymous with security controls and safeguards.
Covert Channel Analysis [CNSSI 4009]	Determination of the extent to which the security policy model and subsequent lower-level program descriptions may allow unauthorized access to information.
Covert Storage Channel [CNSSI 4009]	Covert channel involving the direct or indirect writing to a storage location by one process and the direct or indirect reading of the storage location by another process. Covert storage channels typically involve a finite resource (e.g., sectors on a disk) that is shared by two subjects at different security levels.
Covert Timing Channel [CNSSI 4009]	Covert channel in which one process signals information to another process by modulating its own use of system resources (e.g., central processing unit time) in such a way that this manipulation affects the real response time observed by the second process.
Cross Domain Solution [CNSSI 4009]	A form of controlled interface that provides the ability to manually and/or automatically access and/or transfer information between different security domains.
Cyber Attack [CNSSI 4009]	An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information.
Cyber Security [CNSSI 4009]	The ability to protect or defend the use of cyberspace from cyber attacks.
Cyberspace [CNSSI 4009]	A global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.
Data Mining/Harvesting	An analytical process that attempts to find correlations or patterns in large data sets for the purpose of data or knowledge discovery.

<p>Defense-in-Breadth [CNSSI 4009]</p>	<p>A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or subcomponent life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement).</p>
<p>Defense-in-Depth</p>	<p>Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.</p>
<p>Developer</p>	<p>A general term that includes: (i) developers or manufacturers of information systems, system components, or information system services; (ii) systems integrators; (iii) vendors; and (iv) product resellers. Development of systems, components, or services can occur internally within organizations (i.e., in-house development) or through external entities.</p>
<p>Digital Media</p>	<p>A form of electronic media where data are stored in digital (as opposed to analog) form.</p>
<p>Discretionary Access Control [CNSSI 4009]</p>	<p>An access control policy that is enforced over all subjects and objects in an information system where the policy specifies that a subject that has been granted access to information can do one or more of the following: (i) pass the information to other subjects or objects; (ii) grant its privileges to other subjects; (iii) change security attributes on subjects, objects, information systems, or system components; (iv) choose the security attributes to be associated with newly-created or revised objects; or (v) change the rules governing access control. Mandatory access controls restrict this capability.</p> <p>A means of restricting access to objects (e.g., files, data entities) based on the identity and need-to-know of subjects (e.g., users, processes) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control).</p>
<p>Domain [CNSSI 4009]</p>	<p>An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture. See <i>Security Domain</i>.</p>

<p>Enterprise [CNSSI 4009]</p>	<p>An organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (e.g., budgets), human resources, security, and information systems, information and mission management. See <i>Organization</i>.</p>
<p>Enterprise Architecture [44 U.S.C. Sec. 3601]</p>	<p>A strategic information asset base, which defines the mission; the information necessary to perform the mission; the technologies necessary to perform the mission; and the transitional processes for implementing new technologies in response to changing mission needs; and includes a baseline architecture; a target architecture; and a sequencing plan.</p>
<p>Environment of Operation [NIST SP 800-37]</p>	<p>The physical surroundings in which an information system processes, stores, and transmits information.</p>
<p>Event [CNSSI 4009, Adapted]</p>	<p>Any observable occurrence in an information system.</p>
<p>Executive Agency [41 U.S.C., Sec. 403]</p>	<p>An executive department specified in 5 U.S.C., Sec. 101; a military department specified in 5 U.S.C., Sec. 102; an independent establishment as defined in 5 U.S.C., Sec. 104(1); and a wholly owned Government corporation fully subject to the provisions of 31 U.S.C., Chapter 91.</p>
<p>Exfiltration</p>	<p>The unauthorized transfer of information from an information system.</p>
<p>External Information System (or Component)</p>	<p>An information system or component of an information system that is outside of the authorization boundary established by the organization and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.</p>
<p>External Information System Service</p>	<p>An information system service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system) and for which the organization typically has no direct control over the application of required security controls or the assessment of security control effectiveness.</p>
<p>External Information System Service Provider</p>	<p>A provider of external information system services to an organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges.</p>

External Network	A network not controlled by the organization.
Failover	The capability to switch over automatically (typically without human intervention or warning) to a <u>redundant</u> or standby information system upon the failure or <u>abnormal termination</u> of the previously active system.
Fair Information Practice Principles	Principles that are widely accepted in the United States and internationally as a general framework for privacy and that are reflected in various federal and international laws and policies. In a number of organizations, the principles serve as the basis for analyzing privacy risks and determining appropriate mitigation strategies.
Federal Agency	See <i>Executive Agency</i> .
Federal Enterprise Architecture [FEA Program Management Office]	A business-based framework for government wide improvement developed by the Office of Management and Budget that is intended to facilitate efforts to transform the federal government to one that is citizen-centered, results-oriented, and market-based.
Federal Information System [40 U.S.C., Sec. 11331]	An information system used or operated by an executive agency, by a contractor of an executive agency, or by another organization on behalf of an executive agency.
FIPS-Validated Cryptography	A cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet requirements specified in FIPS Publication 140-2 (as amended). As a prerequisite to CMVP validation, the cryptographic module is required to employ a cryptographic algorithm implementation that has successfully passed validation testing by the Cryptographic Algorithm Validation Program (CAVP). See <i>NSA-Approved Cryptography</i> .
Firmware [CNSSI 4009]	Computer programs and data stored in hardware - typically in read-only memory (ROM) or programmable read-only memory (PROM) - such that the programs and data cannot be dynamically written or modified during execution of the programs.
Guard (System) [CNSSI 4009, Adapted]	A mechanism limiting the exchange of information between information systems or subsystems.
Hardware [CNSSI 4009]	The physical components of an information system. See <i>Software</i> and <i>Firmware</i> .
High-Impact System [FIPS 200]	An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS Publication 199 potential impact value of high.
Hybrid Security Control [CNSSI 4009]	A security control that is implemented in an information system in part as a common control and in part as a system-specific control. See <i>Common Control</i> and <i>System-Specific Security Control</i> .

Impact	The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system.
Impact Value	The assessed potential impact resulting from a compromise of the confidentiality, integrity, or availability of information expressed as a value of low, moderate or high.
Incident [FIPS 200]	An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.
Industrial Control System	An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition (SCADA) systems used to control geographically dispersed assets, as well as distributed control systems (DCSs) and smaller control systems using programmable logic controllers to control localized processes.
Information [CNSSI 4009] [FIPS 199]	Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual. An instance of an information type.
Information Leakage	The intentional or unintentional release of information to an untrusted environment.
Information Owner [CNSSI 4009]	Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information Resources [44 U.S.C., Sec. 3502]	Information and related resources, such as personnel, equipment, funds, and information technology.
Information Security [44 U.S.C., Sec. 3542]	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.
Information Security Architecture	An embedded, integral part of the enterprise architecture that describes the structure and behavior for an enterprise's security processes, information security systems, personnel and organizational subunits, showing their alignment with the enterprise's mission and strategic plans.

Information Security Policy [CNSSI 4009]	Aggregate of directives, regulations, rules, and practices that prescribes how an organization manages, protects, and distributes information.
Information Security Program Plan	Formal document that provides an overview of the security requirements for an organization-wide information security program and describes the program management controls and common controls in place or planned for meeting those requirements.
Information Security Risk	The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information and/or information systems.
Information Steward [CNSSI 4009]	An agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.
Information System [44 U.S.C., Sec. 3502]	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.
Information System Boundary	See <i>Authorization Boundary</i> .
Information System Component [NIST SP 800-128, Adapted]	A discrete, identifiable information technology asset (e.g., hardware, software, firmware) that represents a building block of an information system. Information system components include commercial information technology products.
Information System Owner (or Program Manager)	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.
Information System Resilience	The ability of an information system to continue to: (i) operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities; and (ii) recover to an effective operational posture in a time frame consistent with mission needs.
Information System Security Officer [CNSSI 4009]	Individual with assigned responsibility for maintaining the appropriate operational security posture for an information system or program.
Information System Service	A capability provided by an information system that facilitates information processing, storage, or transmission.

<p>Information System-Related Security Risks</p>	<p>Risks that arise through the loss of confidentiality, integrity, or availability of information or information systems and that considers impacts to the organization (including assets, mission, functions, image, or reputation), individuals, other organizations, and the Nation. See <i>Risk</i>.</p>
<p>Information Technology [40 U.S.C., Sec. 1401]</p>	<p>Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which: (i) requires the use of such equipment; or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term <i>information technology</i> includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.</p>
<p>Information Technology Product</p>	<p>See <i>Information System Component</i>.</p>
<p>Information Type [FIPS 199]</p>	<p>A specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor-sensitive, security management) defined by an organization or in some instances, by a specific law, Executive Order, directive, policy, or regulation.</p>
<p>Insider [Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs]</p>	<p>Any person with authorized access to any U.S. Government resource, to include personnel, facilities, information, equipment, networks, or systems.</p>
<p>Insider Threat [Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs]</p>	<p>The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure of national security information, or through the loss or degradation of departmental resources or capabilities.</p>
<p>[CNSSI 4009]</p>	<p>An entity with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service.</p>

<p>Insider Threat Program [Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs]</p>	<p>A coordinated group of capabilities under centralized management that is organized to detect and prevent the unauthorized disclosure of sensitive information. At a minimum, for departments and agencies that handle classified information, an insider threat program shall consist of capabilities that provide access to information; centralized information integration, analysis, and response; employee insider threat awareness training; and the monitoring of user activity on government computers. For department and agencies that do not handle classified information, these can be employed effectively for safeguarding information that is unclassified but sensitive.</p>
<p>Integrity [44 U.S.C., Sec. 3542]</p>	<p>Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.</p>
<p>Internal Network</p>	<p>A network where: (i) the establishment, maintenance, and provisioning of security controls are under the direct control of organizational employees or contractors; or (ii) cryptographic encapsulation or similar security technology implemented between organization-controlled endpoints, provides the same effect (at least with regard to confidentiality and integrity). An internal network is typically organization-owned, yet may be organization-controlled while not being organization-owned.</p>
<p>Label</p>	<p>See <i>Security Label</i>.</p>
<p>Line of Business</p>	<p>The following OMB-defined process areas common to virtually all federal agencies: Case Management, Financial Management, Grants Management, Human Resources Management, Federal Health Architecture, Information Systems Security, Budget Formulation and Execution, Geospatial, and IT Infrastructure.</p>
<p>Local Access</p>	<p>Access to an organizational information system by a user (or process acting on behalf of a user) communicating through a direct connection without the use of a network.</p>
<p>Logical Access Control System [FICAM Roadmap and Implementation Guidance]</p>	<p>An automated system that controls an individual's ability to access one or more computer system resources such as a workstation, network, application, or database. A logical access control system requires validation of an individual's identity through some mechanism such as a PIN, card, biometric, or other token. It has the capability to assign different access privileges to different persons depending on their roles and responsibilities in an organization.</p>
<p>Low-Impact System [FIPS 200]</p>	<p>An information system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS Publication 199 potential impact value of low.</p>

Malicious Code	Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.
Malware	See <i>Malicious Code</i> .
Managed Interface	An interface within an information system that provides boundary protection capability using automated mechanisms or devices.
Mandatory Access Control [CNSSI 4009]	<p>An access control policy that is uniformly enforced across all subjects and objects within the boundary of an information system. A subject that has been granted access to information is constrained from doing any of the following: (i) passing the information to unauthorized subjects or objects; (ii) granting its privileges to other subjects; (iii) changing one or more security attributes on subjects, objects, the information system, or system components; (iv) choosing the security attributes to be associated with newly-created or modified objects; or (v) changing the rules governing access control. Organization-defined subjects may explicitly be granted organization-defined privileges (i.e., they are trusted subjects) such that they are not limited by some or all of the above constraints.</p> <p>A means of restricting access to objects based on the sensitivity (as represented by a security label) of the information contained in the objects and the formal authorization (i.e., clearance, formal access approvals, and need-to-know) of subjects to access information of such sensitivity. Mandatory Access Control is a type of nondiscretionary access control.</p>
Marking	See <i>Security Marking</i> .
Media [FIPS 200]	Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.
Metadata	Information describing the characteristics of data including, for example, structural metadata describing data structures (e.g., data format, syntax, and semantics) and descriptive metadata describing data contents (e.g., information security labels).
Mobile Code	Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.

<p>Mobile Code Technologies</p>	<p>Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript).</p>
<p>Mobile Device</p>	<p>A portable computing device that: (i) has a small form factor such that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained power source. Mobile devices may also include voice communication capabilities, on-board sensors that allow the devices to capture information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and E-readers.</p>
<p>Moderate-Impact System [FIPS 200]</p>	<p>An information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS Publication 199 potential impact value of moderate and no security objective is assigned a FIPS Publication 199 potential impact value of high.</p>
<p>Multifactor Authentication</p>	<p>Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (e.g., password/PIN); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). See <i>Authenticator</i>.</p>
<p>Multilevel Security [CNSSI 4009]</p>	<p>Concept of processing information with different classifications and categories that simultaneously permits access by users with different security clearances and denies access to users who lack authorization.</p>
<p>Multiple Security Levels [CNSSI 4009]</p>	<p>Capability of an information system that is trusted to contain, and maintain separation between, resources (particularly stored data) of different security domains.</p>
<p>National Security Emergency Preparedness Telecommunications Services [47 C.F.R., Part 64, App A]</p>	<p>Telecommunications services that are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) that causes or could cause injury or harm to the population, damage to or loss of property, or degrade or threaten the national security or emergency preparedness posture of the United States.</p>

<p>National Security System [44 U.S.C., Sec. 3542]</p>	<p>Any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency—(i) the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions (excluding a system that is to be used for routine administrative and business applications, for example, payroll, finance, logistics, and personnel management applications); or (ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.</p>
<p>Network [CNSSI 4009]</p>	<p>Information system(s) implemented with a collection of interconnected components. Such components may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.</p>
<p>Network Access</p>	<p>Access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).</p>
<p>Nondiscretionary Access Control</p>	<p>See <i>Mandatory Access Control</i>.</p>
<p>Nonlocal Maintenance</p>	<p>Maintenance activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network.</p>
<p>Non-Organizational User</p>	<p>A user who is not an organizational user (including public users).</p>
<p>Non-repudiation</p>	<p>Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.</p>
<p>NSA-Approved Cryptography</p>	<p>Cryptography that consists of: (i) an approved algorithm; (ii) an implementation that has been approved for the protection of classified information and/or controlled unclassified information in a particular environment; and (iii) a supporting key management infrastructure.</p>
<p>Object</p>	<p>Passive information system-related entity (e.g., devices, files, records, tables, processes, programs, domains) containing or receiving information. Access to an object (by a subject) implies access to the information it contains. See <i>Subject</i>.</p>

<p>Operations Security [CNSSI 4009]</p>	<p>Systematic and proven process by which potential adversaries can be denied information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities. The process involves five steps: identification of critical information, analysis of threats, analysis of vulnerabilities, assessment of risks, and application of appropriate countermeasures.</p>
<p>Organization [FIPS 200, Adapted]</p>	<p>An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency or, as appropriate, any of its operational elements).</p>
<p>Organizational User</p>	<p>An organizational employee or an individual the organization deems to have equivalent status of an employee including, for example, contractor, guest researcher, individual detailed from another organization. Policy and procedures for granting equivalent status of employees to individuals may include need-to-know, relationship to the organization, and citizenship.</p>
<p>Overlay</p>	<p>A specification of security controls, control enhancements, supplemental guidance, and other supporting information employed during the tailoring process, that is intended to complement (and further refine) security control baselines. The overlay specification may be more stringent or less stringent than the original security control baseline specification and can be applied to multiple information systems.</p>
<p>Penetration Testing</p>	<p>A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.</p>
<p>Personally Identifiable Information [OMB Memorandum 07-16]</p>	<p>Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.).</p>
<p>Physical Access Control System [FICAM Roadmap and Implementation Guidance]</p>	<p>An automated system that manages the passage of people or assets through an opening(s) in a secure perimeter(s) based on a set of authorization rules.</p>
<p>Plan of Action and Milestones [OMB Memorandum 02-01]</p>	<p>A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.</p>

Portable Storage Device	An information system component that can be inserted into and removed from an information system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain non-volatile memory).
Potential Impact [FIPS 199]	The loss of confidentiality, integrity, or availability could be expected to have: (i) a <i>limited</i> adverse effect (FIPS Publication 199 low); (ii) a <i>serious</i> adverse effect (FIPS Publication 199 moderate); or (iii) a <i>severe</i> or <i>catastrophic</i> adverse effect (FIPS Publication 199 high) on organizational operations, organizational assets, or individuals.
Privacy Act Statement	A disclosure statement required by Section (e)(3) of the Privacy Act of 1974, as amended, to appear on documents used by organizations to collect personally identifiable information from individuals to be maintained in a Privacy Act System of Records (SORN).
Privacy Impact Assessment [OMB Memorandum 03-22]	An analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
Privileged Account	An information system account with authorizations of a privileged user.
Privileged Command	A human-initiated command executed on an information system involving the control, monitoring, or administration of the system including security functions and associated security-relevant information.
Privileged User [CNSSI 4009]	A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.
Protective Distribution System	Wire line or fiber optic system that includes adequate safeguards and/or countermeasures (e.g., acoustic, electric, electromagnetic, and physical) to permit its use for the transmission of unencrypted information.
Provenance	The records describing the possession of, and changes to, components, component processes, information, systems, organization, and organizational processes. Provenance enables all changes to the baselines of components, component processes, information, systems, organizations, and organizational processes, to be reported to specific actors, functions, locales, or activities.

Public Key Infrastructure [CNSSI 4009]	The framework and services that provide for the generation, production, distribution, control, accounting, and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates.
Purge	Rendering sanitized data unrecoverable by laboratory attack methods.
Reciprocity [CNSSI 4009]	Mutual agreement among participating organizations to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information.
Records	The recordings (automated and/or manual) of evidence of activities performed or results achieved (e.g., forms, reports, test results), which serve as a basis for verifying that the organization and the information system are performing as intended. Also used to refer to units of related data fields (i.e., groups of data fields that can be accessed by a program and that contain the complete set of information on particular items).
Red Team Exercise	An exercise, reflecting real-world conditions, that is conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization.
Reference Monitor	A set of design requirements on a reference validation mechanism which as key component of an operating system, enforces an access control policy over all subjects and objects. A reference validation mechanism must be: (i) always invoked (i.e., complete mediation); (ii) tamperproof; and (iii) small enough to be subject to analysis and tests, the completeness of which can be assured (i.e., verifiable).
Remote Access	Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).
Remote Maintenance	Maintenance activities conducted by individuals communicating through an external network (e.g., the Internet).
Resilience	See <i>Information System Resilience</i> .

<p>Restricted Data [Atomic Energy Act of 1954]</p>	<p>All data concerning (i) design, manufacture, or utilization of atomic weapons; (ii) the production of special nuclear material; or (iii) the use of special nuclear material in the production of energy, but shall not include data declassified or removed from the Restricted Data category pursuant to Section 142 [of the Atomic Energy Act of 1954].</p>
<p>Risk [FIPS 200, Adapted]</p>	<p>A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.</p> <p>Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.</p>
<p>Risk Assessment</p>	<p>The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system.</p> <p>Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.</p>
<p>Risk Executive (Function) [CNSSI 4009]</p>	<p>An individual or group within an organization that helps to ensure that: (i) security risk-related considerations for individual information systems, to include the authorization decisions for those systems, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and (ii) managing risk from individual information systems is consistent across the organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success.</p>
<p>Risk Management [CNSSI 4009, adapted]</p>	<p>The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.</p>
<p>Risk Mitigation [CNSSI 4009]</p>	<p>Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.</p>

Risk Monitoring	Maintaining ongoing awareness of an organization’s risk environment, risk management program, and associated activities to support risk decisions.
Risk Response	Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation.
Role-Based Access Control	Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.
Safeguards [CNSSI 4009]	Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.
Sanitization	<p>Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means.</p> <p>Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.</p>
Scoping Considerations	A part of tailoring guidance providing organizations with specific considerations on the applicability and implementation of security controls in the security control baseline. Areas of consideration include policy/regulatory, technology, physical infrastructure, system component allocation, operational/environmental, public access, scalability, common control, and security objective.
Security [CNSSI 4009]	A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise’s risk management approach.
Security Assessment	See <i>Security Control Assessment</i> .
Security Assessment Plan	The objectives for the security control assessment and a detailed roadmap of how to conduct such an assessment.

Security Assurance	See <i>Assurance</i> .
Security Attribute	An abstraction representing the basic properties or characteristics of an entity with respect to safeguarding information; typically associated with internal data structures (e.g., records, buffers, files) within the information system and used to enable the implementation of access control and flow control policies, reflect special dissemination, handling or distribution instructions, or support other aspects of the information security policy.
Security Authorization	See <i>Authorization</i> .
Security Authorization Boundary	See <i>Authorization Boundary</i> .
Security Capability	A combination of mutually reinforcing security controls (i.e., safeguards and countermeasures) implemented by technical means (i.e., functionality in hardware, software, and firmware), physical means (i.e., physical devices and protective measures), and procedural means (i.e., procedures performed by individuals).
Security Categorization	The process of determining the security category for information or an information system. Security categorization methodologies are described in CNSS Instruction 1253 for national security systems and in FIPS Publication 199 for other than national security systems. See <i>Security Category</i> .
Security Category [FIPS 199, Adapted; CNSSI 4009]	The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, individuals, other organizations, and the Nation.
Security Control [FIPS 199, Adapted]	A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.
Security Control Assessment [CNSSI 4009, Adapted]	The testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.
Security Control Assessor	The individual, group, or organization responsible for conducting a security control assessment.
Security Control Baseline [FIPS 200, Adapted]	The set of minimum security controls defined for a low-impact, moderate-impact, or high-impact information system that provides a starting point for the tailoring process.

Security Control Enhancement	Augmentation of a security control to: (i) build in additional, but related, functionality to the control; (ii) increase the strength of the control; or (iii) add assurance to the control.
Security Control Inheritance [CNSSI 4009]	A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See <i>Common Control</i> .
Security Control Overlay	See <i>Overlay</i> .
Security Domain [CNSSI 4009]	A domain that implements a security policy and is administered by a single authority.
Security Functionality	The security-related features, functions, mechanisms, services, procedures, and architectures implemented within organizational information systems or the environments in which those systems operate.
Security Functions	The hardware, software, and/or firmware of the information system responsible for enforcing the system security policy and supporting the isolation of code and data on which the protection is based.
Security Impact Analysis [CNSSI 4009]	The analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.
Security Incident	See <i>Incident</i> .
Security Kernel [CNSSI 4009]	Hardware, firmware, and software elements of a trusted computing base implementing the reference monitor concept. Security kernel must mediate all accesses, be protected from modification, and be verifiable as correct.
Security Label	The means used to associate a set of security attributes with a specific information object as part of the data structure for that object.
Security Marking	The means used to associate a set of security attributes with objects in a human-readable form, to enable organizational process-based enforcement of information security policies.
Security Objective [FIPS 199]	Confidentiality, integrity, or availability.
Security Plan	Formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. See <i>System Security Plan</i> or <i>Information Security Program Plan</i> .

<p>Security Policy [CNSSI 4009]</p>	<p>A set of criteria for the provision of security services.</p>
<p>Security Policy Filter</p>	<p>A hardware and/or software component that performs one or more of the following functions: (i) content verification to ensure the data type of the submitted content; (ii) content inspection, analyzing the submitted content to verify it complies with a defined policy (e.g., allowed vs. disallowed file constructs and content portions); (iii) malicious content checker that evaluates the content for malicious code; (iv) suspicious activity checker that evaluates or executes the content in a safe manner, such as in a sandbox/detonation chamber and monitors for suspicious activity; or (v) content sanitization, cleansing, and transformation, which modifies the submitted content to comply with a defined policy.</p>
<p>Security Requirement [FIPS 200, Adapted]</p>	<p>A requirement levied on an information system or an organization that is derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, and/or mission/business needs to ensure the confidentiality, integrity, and availability of information that is being processed, stored, or transmitted.</p> <p>Note: Security requirements can be used in a variety of contexts from high-level policy-related activities to low-level implementation-related activities in system development and engineering disciplines.</p>
<p>Security Service [CNSSI 4009]</p>	<p>A capability that supports one, or more, of the security requirements (Confidentiality, Integrity, Availability). Examples of security services are key management, access control, and authentication.</p>
<p>Security-Relevant Information</p>	<p>Any information within the information system that can potentially impact the operation of security functions or the provision of security services in a manner that could result in failure to enforce the system security policy or maintain isolation of code and data.</p>
<p>Senior Agency Information Security Officer [44 U.S.C., Sec. 3544]</p>	<p>Official responsible for carrying out the Chief Information Officer responsibilities under FISMA and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers.</p> <p>Note: Organizations subordinate to federal agencies may use the term <i>Senior Information Security Officer</i> or <i>Chief Information Security Officer</i> to denote individuals filling positions with similar responsibilities to Senior Agency Information Security Officers.</p>
<p>Senior Agency Official for Privacy</p>	<p>The senior organizational official with overall organization-wide responsibility for information privacy issues.</p>

Senior Information Security Officer	See <i>Senior Agency Information Security Officer</i> .
Sensitive Information [CNSSI 4009, Adapted]	Information where the loss, misuse, or unauthorized access or modification could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act); that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.
Sensitive Compartmented Information [CNSSI 4009]	Classified information concerning or derived from intelligence sources, methods, or analytical processes, which is required to be handled within formal access control systems established by the Director of National Intelligence.
Service-Oriented Architecture	A set of principles and methodologies for designing and developing software in the form of interoperable services. These services are well-defined business functions that are built as software components (i.e., discrete pieces of code and/or data structures) that can be reused for different purposes.
Software [CNSSI 4009]	Computer programs and associated data that may be dynamically written or modified during execution.
Spam	The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.
Special Access Program [CNSSI 4009]	A program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for information at the same classification level.
Spyware	Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.
Subject	Generally, an individual, process, or device causing information to flow among objects or change to the system state. See <i>Object</i> .
Subsystem	A major subdivision or component of an information system consisting of information, information technology, and personnel that performs one or more specific functions.
Supplemental Guidance	Statements used to provide additional explanatory information for security controls or security control enhancements.
Supplementation	The process of adding security controls or control enhancements to a security control baseline as part of the tailoring process (during security control selection) in order to adequately meet the organization's risk management needs.

Supply Chain [ISO 28001, Adapted]	Linked set of resources and processes between multiple tiers of developers that begins with the sourcing of products and services and extends through the design, development, manufacturing, processing, handling, and delivery of products and services to the acquirer.
Supply Chain Element	An information technology product or product component that contains programmable logic and that is critically important to the functioning of an information system.
System	See <i>Information System</i> .
System of Records Notice	An official public notice of an organization's system(s) of records, as required by the Privacy Act of 1974, that identifies: (i) the purpose for the system of records; (ii) the individuals covered by information in the system of records; (iii) the categories of records maintained about individuals; and (iv) the ways in which the information is shared.
System Security Plan [NIST SP 800-18]	Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.
System-Specific Security Control	A security control for an information system that has not been designated as a common security control or the portion of a hybrid control that is to be implemented within an information system.
Tailored Security Control Baseline	A set of security controls resulting from the application of tailoring guidance to a security control baseline. See <i>Tailoring</i> .
Tailoring	The process by which security control baselines are modified by: (i) identifying and designating common controls; (ii) applying scoping considerations on the applicability and implementation of baseline controls; (iii) selecting compensating security controls; (iv) assigning specific values to organization-defined security control parameters; (v) supplementing baselines with additional security controls or control enhancements; and (vi) providing additional specification information for control implementation.
Threat [CNSSI 4009, Adapted]	Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.
Threat Assessment [CNSSI 4009]	Formal description and evaluation of threat to an information system.

Threat Source [FIPS 200]	The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability. Synonymous with threat agent.
Trusted Path	A mechanism by which a user (through an input device) can communicate directly with the security functions of the information system with the necessary confidence to support the system security policy. This mechanism can only be activated by the user or the security functions of the information system and cannot be imitated by untrusted software.
Trustworthiness [CNSSI 4009]	The attribute of a person or enterprise that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities.
Trustworthiness (Information System)	The degree to which an information system (including the information technology components that are used to build the system) can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system across the full range of threats. A trustworthy information system is a system that is believed to be capable of operating within defined levels of risk despite the environmental disruptions, human errors, structural failures, and purposeful attacks that are expected to occur in its environment of operation.
User [CNSSI 4009, adapted]	Individual, or (system) process acting on behalf of an individual, authorized to access an information system. <i>See Organizational User and Non-Organizational User.</i>
Virtual Private Network [CNSSI 4009]	Protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line.
Vulnerability [CNSSI 4009]	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
Vulnerability Analysis	<i>See Vulnerability Assessment.</i>
Vulnerability Assessment [CNSSI 4009]	Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.
Whitelisting	The process used to identify: (i) software programs that are authorized to execute on an information system; or (ii) authorized Universal Resource Locators (URL)/websites.

Appendix B: Acronyms

COMMON ABBREVIATIONS

APT	Advanced Persistent Threat
CFR	Code of Federal Regulations
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CAVP	Cryptographic Algorithm Validation Program
CMVP	Cryptographic Module Validation Program
CNSS	Committee on National Security Systems
CPO	Chief Privacy Officer
CUI	Controlled Unclassified Information
DCS	Distributed Control System
DNS	Domain Name System
DoD	Department of Defense
FAR	Federal Acquisition Regulation
FEA	Federal Enterprise Architecture
FICAM	Federal Identity, Credential, and Access Management
FIPP	Fair Information Practice Principles
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
HSPD	Homeland Security Presidential Directive
ICS	Industrial Control System
IEEE	Institute of Electrical and Electronics Engineers
IPsec	Internet Protocol Security
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
ITL	Information Technology Laboratory
LACS	Logical Access Control System
LSI	Large-Scale Integration
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency or Internal Report
NSA	National Security Agency

NSTISSI	National Security Telecommunications and Information System Security Instruction
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OPSEC	Operations Security
PBX	Private Branch Exchange
PACS	Physical Access Control System
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RBAC	Role-Based Access Control
RD	Restricted Data
RMF	Risk Management Framework
SAISO	Senior Agency Information Security Officer
SAMI	Sources And Methods Information
SAOP	Senior Agency Official for Privacy
SAP	Special Access Program
SC	Security Category
SCADA	Supervisory Control and Data Acquisition
SCI	Sensitive Compartmented Information
SOA	Service-Oriented Architecture
SORN	System of Records Notice
SP	Special Publication
TCP/IP	Transmission Control Protocol/Internet Protocol
USB	Universal Serial Bus
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network

Appendix C: Department Listing

Department	Department Code
Agricultural Commissioner	AG
Airport	AIR
Assessor/Recorder/County Clerk	ARCC
Auditor Controller	ACO
Board of Supervisors	BOS
Child Support Services	DCSS
Community Development Services	CDD
County Administrator	CAO
County Counsel	CC
District Attorney	DA
Employment-Economic Development	EEDD
Environmental Health	EHD
General Services	GSD
Health Care Services Admin	HCSA
San Joaquin Health	SJC
General Hospital	SJGH
Human Resources	HR
Human Services Agency	HSA
OES	OES
Probation Administration	PROB
Public Defender	PD
Public Works	PW
Purchasing - Support Services	PUR
Registrar of Voters	ROV
Sheriff Admin Support Services	SO
Treasurer-Tax Collector	TTC
UC Cooperative Extension	UCE

Behavioral Health Services	BHS
Correctional Health Services	CHS
Emergency Medical Services Administration	EMSA
Office of Medical Examiner	OME
Public Health Services	PHS
Veterans Services Officer	VSO
Neighborhood Preservation	NP
Information Systems Division ISF	ISD
Radio ISF	RAD
Telephone ISF	TEL

Appendix D: Device Type Listing

Device Type	Device Type Code
Desktop Computers	WRK
Laptop Computers	LAP
Tablets (iPads and Android devices)	TAB
Mobile/Smart Phones (basic cell phones, iPhones, BlackBerry, Windows, and Android Phones)	MOB
Servers	S
External Storage Devices	EXT
Network Switches	NET
Routers	R
Firewalls	FW
Security Appliances	SA
Internet of Things (IoT) devices	IOT
Operational Technology (OT) devices	OT
Printers	P
Scanners	C
Kiosks and Thin clients	K
Mainframe Hardware	M
Telephones (VoIP)	VOIP

Appendix E: Security and Privacy Control Catalog Compliance Mapping

System Security Risk Management Plan Security Control		SJC Information Security Policy	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	CIS Critical Security Controls (v8)	IRS Publication 1075 Controls	HIPAA Security Controls (45 CFR Parts 164) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
Access Control Family							
AC-1	Access Control Policy and Procedures	<u>Access Control Policy</u>	5360 Identity and Access Management		9.3.1.1 Access Control Policy and Procedures	164.308(a)(3)(i), 164.308(a)(3)(ii)(A), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.312(a)(1)	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.15, A.5.2, A.5.31, A.5.36, A.5.37, A.5.4
AC-2	Account Management	<u>Access Control Policy</u>	5315.8 Information Asset Connections 5335 Information Security Monitoring 5360 Identity and Access Management	Control 4, 4.3: Configure Automatic Session Locking on Enterprise Assets Control 5, 5.3: Disable Dormant Accounts, 5.6: Centralize Account Management Control 6, 6.1: Establish an Access Granting Process, 6.2: Establish an Access Revoking Process, 6.7: Centralize Access Control Control 12, 12.5: Centralize Network Authentication, Authorization, and Auditing (AAA)	9.3.1.2 Account Management	164.308(a)(3), 164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C), 164.308(a)(5)(ii)(C), 164.312(a)(2)(i), 164.312(a)(2)(ii)	A.5.16, A.5.18, A.8.2

System Security Risk Management Plan Security Control		SJC Information Security Policy	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	CIS Critical Security Controls (v8)	IRS Publication 1075 Controls	HIPAA Security Controls (45 CFR Parts 164) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
AC-3	Access Enforcement	Access Control Policy	5350.1 Encryption 5360 Identity and Access Management		9.3.1.3 Access Enforcement	164.308(a)(3) 164.308(a)(3)(ii)(A), 164.308(a)(4)(ii)(B), 164.310(b), 164.312(a) 164.312(a)(2)(i), 164.312(a)(2)(ii)	A.5.15, A.5.33, A.8.18, A.8.20, A.8.26, A.8.3, A.8.4
AC-4	Information Flow Enforcement		5315.8 Information Asset Connections 5360 Identity and Access Management	Control 3, 3.8: Document Data Flows	9.3.1.4 Information Flow Enforcement	164.308(a)(3)(ii)(A), 164.308(a)(4)(ii)(B), 164.310(b)	A.5.14, A.8.22, A.8.23
AC-5	Separation of Duties	Access Control Policy	5360 Identity and Access Management	Control 3,3.3: Configure Data Access Control Lists Control 6, 6.8: Define and Maintain Role-Based Access Control	9.3.1.5 Separation of Duties	164.308(a)(3)(i), 164.308(a)(4)(i), 164.308(a)(4)(ii)(A), 164.312(a)	A.5.3
AC-6	Least Privilege	Access Control Policy	5360 Identity and Access Management	Control 3, 3.3: Configure Data Access Control Lists, 3.14: Log Sensitive Data Access Control 5, 5.4: Restrict Administrator Privileges to Dedicated Administrator Accounts	9.3.1.6 Least Privilege	164.308(a)(3)(i), 164.308(a)(4)(i), 164.308(a)(4)(ii)(A), 164.312(a)	A.5.15, A.8.18, A.8.2
AC-7	Unsuccessful Logon Attempts	Access Control Policy	5335 Information Security Monitoring 5335.2 Auditable Events 5360 Identity and Access Management		9.3.1.7 Unsuccessful Logon Attempts		A.8.5
AC-8	System Use Notification	Access Control Policy	5360 Identity and Access Management				A.8.5
AC-9	Previous Logon (Access) Notification						A.8.5
AC-10	Concurrent Session Control						
AC-11	Session Lock	Access Control Policy	5360 Identity and Access Management	Control 4, Safeguard 4.3: Configure Automatic Session Locking on Enterprise Assets	9.3.1.9 Session Lock	164.310(b)	A.7.7 A.8.1
AC-12	Session Termination	Access Control Policy	5360 Identity and Access Management	Control 4, Safeguard 4.3: Configure Automatic Session Locking on Enterprise Assets	9.3.1.10 Session Termination	164.310(b), 164.312(a)(2)(iii)	

System Security Risk Management Plan Security Control		SJC Information Security Policy	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	CIS Critical Security Controls (v8)	IRS Publication 1075 Controls	HIPAA Security Controls (45 CFR Parts 164) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
AC-14	Permitted Actions without Identification or Authentication		5360 Identity and Access Management		9.3.1.11 Permitted Actions without Identification or Authentication	164.312(a)(2)(ii)	None
AC-17	Remote Access	<u>Access Control Policy</u>	5315.8 Information Asset Connections 5360 Identity and Access Management 5360.1 Remote Access	Control 12, 12.7: Ensure Remote Devices Utilize a VPN and are Connecting to an Enterprise's AAA Infrastructure, 12.8: Establish and Maintain Dedicated Computing Resources for All Administrative Work Control 13, 13.5: Manage Access Control for Remote Assets	9.3.1.12 Remote Access 4.0 Secure Storage—IRC 6103(p)(4)(B); (4.7 Telework Locations)	164.310(b)	A.5.14 A.6.7
AC-18	Wireless Access	<u>Access Control Policy</u>	5315.8 Information Asset Connections 5360 Identity and Access Management 5360.2 Wireless Access	Control 4, Safeguard 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure	9.3.1.13 Wireless Access	None	A.5.14 A.8.20
AC-19	Access Control for Mobile Devices	<u>Access Control Policy</u>	5315.8 Information Asset Connections 5360 Identity and Access Management	Control 4, Safeguard 4.12: Separate Enterprise Workspaces on Mobile End-User Devices	9.3.1.14 Access Control for Mobile Devices	164.310(b)	A.5.14 A.7.9, A.8.1
AC-20	Use of External Information Systems	<u>Access Control Policy</u>	5315.8 Information Asset Connections 5360 Identity and Access Management	Control 15, 15.3: Classify Service Providers, 15.5: Assess Service Providers	9.3.1.15 Use of External Information Systems	None	A.5.14 A.7.9 A.8.20
AC-21	Information Sharing	<u>Access Control Policy</u>	5315.8 Information Asset Connections 5360 Identity and Access Management	Control 15, 15.2: Establish and Maintain a Service Provider Management Policy	9.3.1.16 Information Sharing Restricting Access—IRC 6103(p)(4)(C); (5.4 Controls over Processing)	None	None
AC-22	Publicly Accessible Content	<u>Access Control Policy</u>	5310 Privacy		9.3.1.17 Publicly Accessible Content	None	None

System Security Risk Management Plan Security Control		SJC Information Security Policy	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	CIS Critical Security Controls (v8)	IRS Publication 1075 Controls	HIPAA Security Controls (45 CFR Parts 164) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
Audit and Accountability Family							
AU-1	Audit and Accountability Policy and Procedures	<u>Auditing and Accountability Policy</u>	5335 Information Security Monitoring 5335.2 Auditable Events		9.3.3.1 Audit and Accountability Policy and Procedures 3.0 Record Keeping Requirement (3.1 General)	164.312(b) 164.316(b)(2)(ii) 164.316(b)(2)(iii)	5.2.5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.31, A.5.36, A.5.37, A.5.4
AU-2	Auditable Events\Event Logging	<u>Auditing and Accountability Policy</u>	5335 Information Security Monitoring 5335.2 Auditable Events		9.3.3.3 Audit Events 3.0 Record Keeping Requirement (3.2 Electronic and Non-Electronic FTI Logs)	164.312(b)	A.8.15
AU-3	Content of Audit Records	<u>Auditing and Accountability Policy</u>	5335 Information Security Monitoring 5335.2 Auditable Events	Control 8, 8.5: Collect Detailed Audit Logs	9.3.3.4 Content of Audit Records 3.0 Record Keeping Requirement (3.2 Electronic and Non-Electronic FTI Logs)	164.312(b)	A.5.28 A.8.15
AU-4	Audit Log Storage Capacity	<u>Auditing and Accountability Policy</u>	5335 Information Security Monitoring 5335.2 Auditable Events		9.3.3.5 Audit Storage Capacity	164.312(b)	A.8.6
AU-5	Response to Audit Logging Process Failures	<u>Auditing and Accountability Policy</u>	5335 Information Security Monitoring 5335.2 Auditable Events		9.3.3.6 Response to Audit Processing Failures	None	None
AU-6	Audit Record Review, Analysis, and Reporting	<u>Auditing and Accountability Policy</u>	5335 Information Security Monitoring 5335.1 Continuous Monitoring	Control 8, 8.9 Centralize Audit Logs, 8.11: Conduct Audit Log Reviews Control 13, 13.1: Centralize Security Event Alerting	9.3.3.7 Audit Review, Analysis, and Reporting	164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(C), 164.312(b)	A.5.25, A.6.8, A.8.15

System Security Risk Management Plan Security Control		SJC Information Security Policy	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	CIS Critical Security Controls (v8)	IRS Publication 1075 Controls	HIPAA Security Controls (45 CFR Parts 164) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
AU-7	Audit Record Reduction and Report Generation	<u>Auditing and Accountability Policy</u>	5335 Information Security Monitoring 5335.1 Continuous Monitoring	Control 8, 8.2: Collect Audit Logs, 8.4: Standardize Time Synchronization, 8.5: Collect Detailed Audit Logs, 8.11: Conduct Audit Log Reviews Control 13, 13.1: Centralize Security Event Alerting	9.3.3.8 Audit Reduction and Report Generation	164.308(a)(1)(ii)(D), 164.312(b)	A.10.10.2, A.13.2.3
AU-8	Time Stamps	<u>Auditing and Accountability Policy</u>	5335 Information Security Monitoring 5335.2 Auditable Events		9.3.3.9 Time Stamps	164.312(b)	A.8.17
AU-9	Protection of Audit Information	<u>Auditing and Accountability Policy</u>	5335 Information Security Monitoring 5335.2 Auditable Events	Control 6, 6.8: Define and Maintain Role-Based Access Control	9.3.3.10 Protection of Audit Information	None	A.5.33 A.8.15
AU-11	Audit Record Retention	<u>Auditing and Accountability Policy</u>	5335 Information Security Monitoring 5335.2 Auditable Events		9.3.3.11 Audit Record Retention (AU-11) 8.0 Disposing of FTI—IRC 6103(p)(4)(F); (General 8.1)	164.316(b)(1), 164.316(b)(2)(i)	A.5.28 A.8.15
AU-12	Audit Generation	<u>Auditing and Accountability Policy</u>	5335 Information Security Monitoring 5335.2 Auditable Events		9.3.3.12 Audit Generation	None	A.8.15
Awareness and Training							
AT-1	Security Awareness and Training Policy and Procedures	<u>Security Awareness and Training Policy</u>				164.308(a)(5) 164.316(b)(2)(ii) 164.316(b)(2)(iii)	5.2,5.3 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.31, A.5.36, A.5.37, A.5.4

System Security Risk Management Plan Security Control		SJC Information Security Policy	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	CIS Critical Security Controls (v8)	IRS Publication 1075 Controls	HIPAA Security Controls (45 CFR Parts 164) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
AT-2	Security Awareness	<u>Security Awareness and Training Policy</u>		Control 14: Train Workforce Members to Recognize Social Engineering Attacks		164.308(a)(5) 164.308(a)(5)(ii)(A) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(D)	7.3, A.6.3, A.8.7
AT-3	Security Training	<u>Security Awareness and Training Policy</u>				164.308(a)(5) 164.308(a)(5)(ii)(A) 164.308(a)(5)(ii)(B) 164.308(a)(5)(ii)(C) 164.308(a)(5)(ii)(D)	A.6.3
AT-4	Training Records					164.308(a)(5)	None
Security Assessment and Authorization Family							
CA-3	System Interconnections\Information Exchange		5305.8 Provisions for Agreements with State and Non-State Entities		9.3.4.3 System Interconnections	164.308(a)(4)(ii)(A) 164.308(b)(1), 164.308(b)(4), 164.314(a)(2)(ii)	A.5.14 A.8.21
CA-5	Plan of Action and Milestones		5300.5 Minimum Security Controls 5330 Information Security Compliance 5330.1 Security Assessments		9.3.4.4 Plan of Action and Milestones 6.0 Other Safeguards—IRC 6103(p)(4)(D);(6.5 Plan of Action and Milestones)		10.2,8.3,9.3.3
CA-6	Security Authorization		5305.8 Provisions for Agreements with State and Non-State Entities 5315.8 Information Asset Connections 5360 Identity and Access Management		9.3.4.5 Security Authorization	164.308(a)(2), 164.308(a)(8)	9.3.1, 9.3.3
CA-7	Continuous Monitoring		5300.5 Minimum Security Controls 5330 Information Security Compliance 5330.1 Security Assessments		9.3.4.6 Continuous Monitoring	164.308(a)(1)(ii)(D), 164.308(a)(8)	9.1, 9.3.2, 9.3.3, A.5.26
CA-8	Penetration testing					164.308(a)(8)	None

System Security Risk Management Plan Security Control		SJC Information Security Policy	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	CIS Critical Security Controls (v8)	IRS Publication 1075 Controls	HIPAA Security Controls (45 CFR Parts 164) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
CA-9	Internal System Connections		5315.8 Information Asset Connections 5360 Identity and Access Management			None	None
Configuration Management Family							
CM-1	Configuration Management Policy and Procedures	<u>Configuration Management Policy</u>	5315.3 Configuration Management	Critical Control 2: Inventory of Authorized and Unauthorized Software. Critical Control 3: Secure Configurations for Hardware and Software. Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches.	9.3.5.1 Configuration Management Policy and Procedures	164.316(b)(2)(ii) 164.316(b)(2)(iii)	5.2.5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.31, A.5.36, A.5.37, A.5.4, A.8.9
CM-2	Baseline Configuration	<u>Configuration Management Policy</u>	5315.6 Activate only Essential Functionality	Control 4: Establish and Maintain a Secure Configuration Process for Network Infrastructure	9.3.5.2 Baseline Configuration		A.8.9
CM-3	Configuration Change Control	<u>Configuration Management Policy</u>	5315.3 Configuration Management		9.3.5.3 Configuration Change Control		8.1, 9.3.3, A.8.32, A.8.9
CM-4	Security Impact Analysis	<u>Configuration Management Policy</u>	5315 Information Security Integration 5315.3 Configuration Management		9.3.5.4 Security Impact Analysis		A.8.9
CM-5	Access Restrictions for Change	<u>Configuration Management Policy</u>	5315.3 Configuration Management		9.3.5.5 Access Restrictions for Change		A.8.9, A.8.2, A.8.31, A.8.32, A.8.4, A.8.9
CM-6	Configuration Settings	<u>Configuration Management Policy</u>	5315.6 Activate only Essential Functionality	Control 4: Establish and Maintain a Secure Configuration Process for Network Infrastructure Control 12: Securely Manage Network Infrastructure	9.3.5.6 Configuration Settings		A.8.9

System Security Risk Management Plan Security Control		SJC Information Security Policy	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	CIS Critical Security Controls (v8)	IRS Publication 1075 Controls	HIPAA Security Controls (45 CFR Parts 164) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
CM-7	Least Functionality	<u>Configuration Management Policy</u>	5315.6 Activate Only Essential Functionality	Control 4: Establish and Maintain a Secure Configuration Process for Network Infrastructure, Establish and Maintain a Secure Configuration Process Control 2: Address Unauthorized Software, Allowlist Authorized Software, Allowlist Authorized Libraries, Allowlist Authorized Scripts Control 12: Securely Manage Network Infrastructure	9.3.5.7 Least Functionality		A.8.19
CM-8	Information System Component Inventory	<u>Configuration Management Policy</u>	5305.5 Information Asset Management	Control 1: 1.1: Establish and Maintain Detailed Enterprise Asset Inventory, 1.2: Address Unauthorized Assets, 1.4: Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory, 1.5: Use a Passive Asset Discovery Tool Control 2, 2.3: Address Unauthorized Software, 2.4: Utilize Automated Software Inventory Tools, 2.5: Allowlist Authorized Software	9.3.5.8 Information System Component Inventory	164.310(d)(1), 164.310(d)(2)(iii)	A.5.9, A.8.9
CM-9	Configuration Management Plan	<u>Configuration Management Policy</u>	5315.3 Configuration Management	Control 4, 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure	9.3.5.9 Configuration Management Plan		A.5.2, A.8.9
CM-10	Software Usage Restrictions	<u>Configuration Management Policy</u>	5315.7 Software Usage Restrictions	Control 2: Address Unauthorized Software Control 9: Restrict Unnecessary or Unauthorized Browser and Email Client Extensions	9.3.5.10 Software Usage Restrictions		A.5.32

System Security Risk Management Plan Security Control		SJC Information Security Policy	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	CIS Critical Security Controls (v8)	IRS Publication 1075 Controls	HIPAA Security Controls (45 CFR Parts 164) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
CM-11	User-Installed Software	<u>Configuration Management Policy</u>	5315.7 Software Usage Restrictions	Control 9: Restrict Unnecessary or Unauthorized Browser and Email Client Extensions	9.3.5.11 User-Installed Software		A.8.19
CM-12	Information Location	<u>Configuration Management Policy</u>		Control 3: Establish and Maintain a Data Management Process, Document Data Flows, Deploy a Data Loss Prevention Solution			
Contingency Planning Family							
CP-1	Contingency Planning Policy and Procedures	<u>Contingency Planning Policy</u>				164.308(a)(7) 164.316(b)(2)(ii) 164.316(b)(2)(iii)	5.2, 5.3., 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.31, A.5.36, A.5.37, A.5.4
CP-2	Contingency Plan	<u>Contingency Planning Policy</u>	5325 Business Continuity with Technology Recovery		9.3.6.2 Contingency Plan	164.308(a)(7), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(D), 164.308(a)(7)(ii)(E), 164.310(a)(2)(i), 164.312(a)(2)(ii)	7.5.1, 7.5.2, 7.5.3, A.5.2, A.5.29, A.8.14
CP-3	Contingency Training	<u>Contingency Planning Policy</u>	5325 Business Continuity with Technology Recovery 5325.2 Technology Recovery Training		9.3.6.3 Contingency Training	164.308(a)(7)(ii)(D)	A.6.3

System Security Risk Management Plan Security Control		SJC Information Security Policy	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	CIS Critical Security Controls (v8)	IRS Publication 1075 Controls	HIPAA Security Controls (45 CFR Parts 164) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
CP-4	Contingency Plan Testing	<u>Contingency Planning Policy</u>	5325 Business Continuity with Technology Recovery 5325.3 Technology Recovery Testing		9.3.6.4 Contingency Plan Testing	164.308(a)(7)(ii)(D)	A.5.29, A.5.30
CP-6	Alternate Storage Site	<u>Contingency Planning Policy</u>	5305.8 Provisions for Agreements with State and Non-State Entities 5325.4 Alternate Storage and Processing Site	Control 11: Establish and Maintain an Isolated Instance of Recovery Data Control 12: Establish and Maintain a Secure Network Architecture	9.3.6.5 Alternate Storage Site Restricting Access—IRC 6103(p)(4)(C); (5.4.2 Contractor- or Agency-Shared Facility—Consolidated Data Centers)	164.308(a)(7)(ii)(B), 164.310(a)(2)(i)	A.5.29, A.7.5, A.8.14
CP-7	Alternate Processing Site	<u>Contingency Planning Policy</u>	5325 Business Continuity with Technology Recovery 5325.4 Alternate Storage and Processing Site	Control 12: Establish and Maintain a Secure Network Architecture	9.3.6.6 Alternate Processing Site	164.308(a)(7)(ii)(B), 164.310(a)(2)(i)	A.5.29*, A.7.5*, A.8.14*
CP-8	Telecommunications Services	<u>Contingency Planning Policy</u>	5305.8 Provisions for Agreements with State and Non-State Entities 5325.5 Telecommunications Services			164.308(a)(7)(ii)(B)	A.5.29*, A.7.11
CP-9	Information System Backup	<u>Contingency Planning Policy</u>	5325.6 Information System Backups	Control 11: Protect Recovery Data, Test Data Recovery	9.3.6.7 Information System Backup	164.308(a)(7)(ii)(A), 164.308(a)(7)(ii)(B), 164.310(d)(2)(iv), 164.312(c)(1)	A.5.29*, A.5.33*, A.8.13
CP-10	Information System Recovery and Reconstitution	<u>Contingency Planning Policy</u>	5325 Business Continuity with Technology Recovery 5325.1 Technology Recovery Plan		9.3.6.8 Information System Recovery and Reconstitution	164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C)	A.5.29*
Identification and Authentication Family							

System Security Risk Management Plan Security Control		SJC Information Security Policy	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	CIS Critical Security Controls (v8)	IRS Publication 1075 Controls	HIPAA Security Controls (45 CFR Parts 164) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
IA-1	Identification and Authentication Policy and Procedures	Identification and Authentication Policy					5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
IA-2	Identification and Authentication (Organizational Users)	Identification and Authentication Policy	5360 Identity and Access Management		9.3.7.2 Identification and Authentication (Organizational Users)	164.308(a)(5)(ii)(D), 164.312(a)(2)(i), 164.312(d)	A.5.16
IA-3	Device Identification and Authentication	Identification and Authentication Policy	5360 Identity and Access Management		9.3.7.3 Device Identification and Authentication	164.312(a)(2)(i), 164.312(d)	None
IA-4	Identifier Management	Identification and Authentication Policy	5360 Identity and Access Management		9.3.7.4 Identifier Management	164.308(a)(5)(ii)(D), 164.312(a)(2)(i), 164.312(d)	A.5.16
IA-5	Authenticator Management	Identification and Authentication Policy	5350.1 Encryption 5360 Identity and Access Management		9.3.7.5 Authenticator Management Secure Storage—IRC 6103(p)(4)(B) Section 4.0	164.308(a)(5)(ii)(D)	A.5.16, A.5.17
IA-6	Authenticator Feedback	Identification and Authentication Policy	5360 Identity and Access Management		9.3.7.6 Authenticator Feedback	164.308(a)(5)(ii)(D)	A.8.5
IA-7	Cryptographic Module Authentication	Identification and Authentication Policy	5350.1 Encryption 5360 Identity and Access Management			164.308(a)(5)(ii)(D)	None
IA-8	Identification and Authentication (Non-Organizational Users)	Identification and Authentication Policy					A.5.16
IA-11	Re-authentication	Identification and Authentication Policy	5360 Identity and Access Management				
Incident Response Family							

System Security Risk Management Plan Security Control		SJC Information Security Policy	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	CIS Critical Security Controls (v8)	IRS Publication 1075 Controls	HIPAA Security Controls (45 CFR Parts 164) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
IR-1	Incident Response Policy and Procedures	<u>Incident Response Policy</u>	5340 Information Security Incident Management		9.3.8.1 Incident Response Policy and Procedures 10.0 Reporting Improper Inspections or Disclosures; (10.1 General)	164.308(a)(6)(i)	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
IR-2	Incident Response Training	<u>Incident Response Policy</u>	5340.1 Incident Response Training		9.3.8.2 Incident Response Training	164.308(a)(6)(i)	A.6.3*
IR-3	Incident Response Testing	<u>Incident Response Policy</u>	5340.2 Incident Response Testing	Control 17: Conduct Routine Incident Response Exercises	9.3.8.3 Incident Response Testing	164.308(a)(6)(i)	None
IR-4	Incident Handling	<u>Incident Response Policy</u>	5340.3 Incident Handling	Control 13: Centralize Security Event Alerting	9.3.8.4 Incident Handling 10.0 Reporting Improper Inspections or Disclosures; (10.2 Office of Safeguards Notification Process)	164.308(a)(6)(ii)	A.5.25, A.5.26, A.5.27
IR-5	Incident Monitoring	<u>Incident Response Policy</u>	5340 Information Security Incident Management		9.3.8.5 Incident Monitoring	164.308(a)(1)(ii)(D), 164.308(a)(6)(ii)	None
IR-6	Incident Reporting	<u>Incident Response Policy</u>	5340.4 Incident Reporting	Control 17: Establish and Maintain Contact Information for Reporting Security Incidents, Establish and Maintain an Enterprise Process for Reporting Incidents, Establish and Maintain an Incident Response Process	9.3.8.6 Incident Reporting 10.0 Reporting Improper Inspections or Disclosures; (10.3 Incident Response Procedures) 10.0 Reporting Improper Inspections or Disclosures; (10.4 Incident Response Notification to Impacted Individuals)	164.308(a)(1)(ii)(D), 164.308(a)(6)(ii), 164.314(a)(2)(i)	A.5.5*, A.6.8
IR-7	Incident Response Assistance	<u>Incident Response Policy</u>	5340 Information Security Incident Management 5340.3 Incident Handling		9.3.8.7 Incident Response Assistance	164.308(a)(6)(ii)	None

System Security Risk Management Plan Security Control		SJC Information Security Policy	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	CIS Critical Security Controls (v8)	IRS Publication 1075 Controls	HIPAA Security Controls (45 CFR Parts 164) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
IR-8	Incident Response Plan	<u>Incident Response Policy</u>	5340 Information Security Incident Management 5340.3 Incident Handling	Control 17: Define Mechanisms for Communicating During Incident Response	9.3.8.8 Incident Response Plan (IR-8) Reporting Improper Inspections or Disclosures Section 10.0 (10.3)		7.5.1, 7.5.2, 7.5.3, A.5.24
Maintenance Family							
MA-1	System Maintenance Policy and Procedures	<u>Maintenance Policy</u>	5315 Information Security Integration		9.3.9.1 System Maintenance Policy and Procedures	164.310(a)(2)(iv)	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.37, A.18.1.1, A.18.2.2
MA-2	Controlled Maintenance	<u>Maintenance Policy</u>	5315 Information Security Integration		9.3.9.2 Controlled Maintenance	164.310(a)(2)(iv)	A.7.10*, A.7.13*, A.8.10*
MA-3	Maintenance Tools	<u>Maintenance Policy</u>	5315 Information Security Integration	Control 2: Establish and Maintain a Software Inventory	9.3.9.3 Maintenance Tools		None
MA-4	Nonlocal Maintenance	<u>Maintenance Policy</u>	5315 Information Security Integration		9.3.9.4 Non-Local Maintenance		None
MA-5	Maintenance Personnel	<u>Maintenance Policy</u>	5315 Information Security Integration		9.3.9.5 Maintenance Personnel	164.308(a)(3)(ii)(A)	None
MA-6	Timely Maintenance	<u>Maintenance Policy</u>	5315 Information Security Integration			164.310(a)(2)(iv)	A.7.13
Media Protection Family							
MP-1	Media Protection Policy and Procedures	<u>Media Protection Policy</u>	5350.1 Encryption 5365.2 Media Protection		9.3.10.1 Media Protection Policy and Procedures Secure Storage—IRC 6103(p)(4)(B) Section 4.0	164.310(d)(1)	5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
MP-2	Media Access		5350.1 Encryption 5365.2 Media Protection	Critical Control 17: Data Loss Prevention	9.3.10.2 Media Access	164.308(a)(3)(ii)(A), 164.310(c), 164.310(d)(1), 164.312(c)(1)	A.5.10*, A.7.7*, A.7.10*

System Security Risk Management Plan Security Control		SJC Information Security Policy	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	CIS Critical Security Controls (v8)	IRS Publication 1075 Controls	HIPAA Security Controls (45 CFR Parts 164) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
MP-3	Media Marking	Media Protection Policy	5365.2 Media Protection	Critical Control 15: Controlled Access Based on the Need to Know	9.3.10.3 Media Marking 5.0 Restricting Access—IRC 6103(p)(4)©; (5.1)	164.310(c , 164.310(d)(1)	A.5.13
MP-4	Media Storage	Media Protection Policy	5350.1 Encryption 5365.2 Media Protection	Critical Control 17: Data Loss Prevention	9.3.10.4 Media Storage 4.0 Secure Storage—IRC 6103(p)(4)(B); (4.6 Media Off-Site Storage Requirements)	164.310(c, 164.310(d)(1), 164.310(d)(2)(iv)	A.5.10*, A.7.7*, A.7.10, A.8.10*
MP-5	Media Transport Custodians	Media Protection Policy	5350.1 Encryption 5365.2 Media Protection	Control 3: Encrypt Data on Removable Media	9.3.10.5 Media Transport 4.0 Secure Storage—IRC 6103(p)(4)(B); (4.6 Media Off-Site Storage Requirements)	164.310(d)(1), 164.310(d)(2)(iii), 164.312(c)(1)	A.5.10*, A.7.9, A.7.10
MP-6	Media Sanitization	Media Protection Policy	5365.3 Media Disposal		9.3.10.6 Media Sanitization (MP-6) 3.0 Record Keeping Requirement (3.3 Converted Media) 8.0 Disposing of FTI—IRC 6103(p)(4)(F); (8.3 Destruction and Disposal)	164.310(d)(1), 164.310(d)(2)(i), 164.310(d)(2)(ii)	A.5.10, A.7.10*, A.7.14, A.8.10
MP-7	Media Use	Media Protection Policy	5365.2 Media Protection				A.5.10, A.7.10
Physical and Environmental Protection Family							
PE-1	Physical and Environment Protection Policy and Procedures	Physical and Environmental Protection Policy					5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
PE-2	Physical Access Authorizations	Physical and Environmental Protection Policy	5335 Information Security Monitoring 5365 Physical Security		9.3.11.2 Physical Access Authorizations Secure Storage—IRC 6103(p)(4)(B) Section 4.0	164.310(a)(1), 164.310(a)(2)(iii)	A.7.2*

System Security Risk Management Plan Security Control		SJC Information Security Policy	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	CIS Critical Security Controls (v8)	IRS Publication 1075 Controls	HIPAA Security Controls (45 CFR Parts 164) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
PE-3	Physical Access Control	<u>Physical and Environmental Protection Policy</u>	5365 Physical Security		9.3.11.3 Physical Access Control (PE-3) Secure Storage—IRC 6103(p)(4)(B) Section 4.0; (4.3) 4.0 Secure Storage—IRC 6103(p)(4)(B); (4.5 Physical Security of Computers, Electronic, and Removable Media)	164.310(a)(1), 164.310(a)(2)(iii), 164.310(b), 164.310(c)	A.7.1, A.7.2, A.7.3, A.7.4
PE-4	Access Control for Transmission Medium	<u>Physical and Environmental Protection Policy</u>	5365 Physical Security		9.3.11.4 Access Control for Transmission Medium	164.310(a)(1), 164.310(c)	A.7.2, A.7.12
PE-5	Access Control for Output Devices	<u>Physical and Environmental Protection Policy</u>	5365 Physical Security 5365.1 Access Control for Output Devices		9.3.11.5 Access Control for Output Devices	164.310(a)(1), 164.310(b), 164.310(c)	A.7.2, A.7.3, A.7.7
PE-6	Monitoring Physical Access	<u>Physical and Environmental Protection Policy</u>	5335 Information Security Monitoring 5335.1 Continuous Monitoring 5335.2 Auditable Events 5365 Physical Security		9.3.11.6 Monitoring Physical Access Secure Storage—IRC 6103(p)(4)(B) Section 4.0 (4.5)	164.310(a)(2)(iii)	A.7.4, A.8.16*
PE-8	Visitor Access Records	<u>Physical and Environmental Protection Policy</u>	5335 Information Security Monitoring 5335.1 Continuous Monitoring 5335.2 Auditable Events 5365 Physical Security	Control 12: Establish and Maintain a Secure Network Architecture	9.3.11.7 Visitor Access Records	164.310(a)(2)(iii)	None
PE-9	Power Equipment and Cabling	<u>Physical and Environmental Protection Policy</u>	5300.5 Minimum Security Controls 5365 Physical Security		Secure Storage—IRC 6103(p)(4)(B); (4.7.1 Equipment)		A.7.5, A.7.8, A.7.11, A.7.12
PE-11	Emergency Power	<u>Physical and Environmental Protection Policy</u>	5300.5 Minimum Security Controls 5365 Physical Security				A.7.11

System Security Risk Management Plan Security Control		SJC Information Security Policy	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	CIS Critical Security Controls (v8)	IRS Publication 1075 Controls	HIPAA Security Controls (45 CFR Parts 164) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
PE-12	Emergency Lighting	<u>Physical and Environmental Protection Policy</u>	5300.5 Minimum Security Controls 5365 Physical Security				A.7.11
PE-13	Fire Protection	<u>Physical and Environmental Protection Policy</u>	5300.5 Minimum Security Controls 5365 Physical Security				A.7.5, A.7.8
PE-14	Temperature and Humidity Controls	<u>Physical and Environmental Protection Policy</u>	5300.5 Minimum Security Controls 5335.1 Continuous Monitoring 5365 Physical Security				A.7.5, A.7.8, A.7.11
PE-15	Water Damage Protection	<u>Physical and Environmental Protection Policy</u>	5300.5 Minimum Security Controls 5335.1 Continuous Monitoring 5365 Physical Security				A.7.5, A.7.8, A.7.11
PE-16	Delivery and Removal	<u>Physical and Environmental Protection Policy</u>	5365 Physical Security		9.3.11.8 Delivery and Removal		A.5.10, A.7.2, A.7.10*
PE-17	Alternate Work Site	<u>Physical and Environmental Protection Policy</u>	5365 Physical Security		9.3.11.9 Alternate Work Site	164.310(a)(2)(i)	A.5.14, A.6.7, A.7.9
PE-19	Information Leakage	<u>Physical and Environmental Protection Policy</u>	5365 Physical Security				A.7.5, A.7.8, A.8.12
Planning Family							
PL-1	Security Planning Policy and Procedures						5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
PL-4	Rules of Behavior		5305.8 Provisions for Agreements with State and Non-State Entities		9.3.12.3 Rules of Behavior		A.5.4, A.5.10, A.6.2

System Security Risk Management Plan Security Control		SJC Information Security Policy	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	CIS Critical Security Controls (v8)	IRS Publication 1075 Controls	HIPAA Security Controls (45 CFR Parts 164) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
PL-8	Information Security and Privacy Architecture		5315 Information Security Integration	Control 12: Establish and Maintain a Secure Network Architecture, Establish and Maintain Architecture Diagram(s) Control 16: Apply Secure Design Principles in Application Architectures			A.5.8
Personnel Security							
PS-1	Personnel Security Policy and Procedures	<u>Personnel Security Policy</u>					5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
PS-2	Position Categorization	<u>Personnel Security Policy</u>					None
PS-3	Personnel Screening	<u>Personnel Security Policy</u>					A.6.1
PS-4	Personnel Termination	<u>Personnel Security Policy</u>	5305.4 Personnel Management		9.3.13.4 Termination	164.308(a)(3)(ii)(C)	A.5.11, A.6.5
PS-5	Personnel Transfer	<u>Personnel Security Policy</u>	5305.4 Personnel Management		9.3.13.5 Personnel Transfer	164.308(a)(3)(ii)(C)	A.5.11, A.6.5
PS-6	Access Agreements	<u>Personnel Security Policy</u>	5305.4 Personnel Management 5315 Information Security Integration		9.3.13.6 Access Agreements (PS-6) 11.0 Disclosure to Other Persons; (11.2 Authorized Disclosures Precautions) 11.0 Disclosure to Other Persons; (11.3 Disclosing FTI to Contractors)	164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(4)(ii)(B), 164.310(b), 164.310(d)(2)(iii), 164.314(a)(1), 164.314(a)(2)(i), 164.314(a)(2)(ii)	A.5.4, A.6.2, A.6.6

System Security Risk Management Plan Security Control		SJC Information Security Policy	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	CIS Critical Security Controls (v8)	IRS Publication 1075 Controls	HIPAA Security Controls (45 CFR Parts 164) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
PS-7	Third-Party Personnel Security	<u>Personnel Security Policy</u>				164.308(a)(3)(ii)(A) 164.308(a)(3)(ii)(B) 164.308(a)(4)(ii)(B) 164.308(b)(1) 164.314(a)(2)(i) 164.314(a)(2)(ii) 164.314(a)(2)(iii)	A.5.2, A.5.4
PS-8	Personnel Sanctions					164.308(a)(1)(ii)(C)	7.3, A.6.4
Personally Identifiable Information Processing and Transparency							
PT-1	Personally Identifiable Information Processing and Transparency Policy and Procedures						A.5.4
PT-2	Authority to prove personally identifiable information						None
PT-3	Personally Identifiable Information Processing Purpose						None
PT-4	Consent						None
PT-5	Privacy Notice						None
PT-6	System of Records Notice						None
Program Management							
PM-1							4.1, 4.2, 4.3, 4.4, 5.2, 5.3, 6.1.1, 6.2, 7.4, 7.5.1, 7.5.2, 7.5.3, 8.1, 9.3.1, 10.1, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36
PM-3	Information Security and Privacy Resources						5.1, 6.2, 7.1
PM-5	System Inventory						None
PM-19	Privacy Program Leadership Role						None

System Security Risk Management Plan Security Control		SJC Information Security Policy	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	CIS Critical Security Controls (v8)	IRS Publication 1075 Controls	HIPAA Security Controls (45 CFR Parts 164) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
PM-20	Dissemination of Privacy Program Information						None
PM-21	Accounting of Disclosures						None
PM-22	Personally Identifiable Information Quality Management						None
PM-25	Minimization of Personally Identifiable Information used in Testing, Training and Research						None
PM-26	Compliant Management						None
PM-27	Privacy Reporting						None
Risk Assessment Family							
RA-1	Risk Assessment Policy and Procedures	<u>Risk Assessment Policy</u>					5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
RA-2	Security Categorization					164.308(a)(1)(ii)(A) 164.308(a)(1)(ii)(B) 164.308(a)(7)(ii)(E)	A.5.12
RA-3	Risk Assessment	<u>Risk Assessment Policy</u>					6.1.2, 8.2, 9.3.2, A.8.8
RA-5	Vulnerability Scanning	<u>Risk Assessment Policy</u>	5330.1 Security Assessments 5335 Information Security Monitoring 5335.1 Continuous Monitoring 5345 Vulnerability and Threat Management		9.3.14.3 Vulnerability Scanning		A.8.8
RA-8	Privacy Impact Assessment						None
System and Services Acquisition Family							

System Security Risk Management Plan Security Control		SJC Information Security Policy	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	CIS Critical Security Controls (v8)	IRS Publication 1075 Controls	HIPAA Security Controls (45 CFR Parts 164) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
SA-1	System and Services Acquisition Policy and Procedures	Information System and Services Acquisition Policy					5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, 8.1, A.5.1, A.5.2, A.5.4, A.5.23, A.5.31, A.5.36, A.5.37
SA-2	Allocation of resources	Information System and Services Acquisition Policy					None
SA-3	System Development Life Cycle	Information System and Services Acquisition Policy	5315 Information Security Integration 5315.2 System Development Lifecycle		9.3.15.3 System Development Life Cycle		A.5.2, A.5.8, A.8.25, A.8.31
SA-4	Acquisition Process	Information System and Services Acquisition Policy	5305.8 Provisions for Agreements with State and Non-State Entities 5315 Information Security Integration 5315.1 System and Services Acquisition		9.3.15.4 Acquisition Process	164.314(a)(2)(i)	8.1, A.5.8, A.5.20, A.5.23, A.8.29, A.8.30
SA-5	Information System Documentation	Information System and Services Acquisition Policy	5315 Information Security Integration 5315.3 Information Asset Documentation		9.3.15.5 Information System Documentation		7.5.1, 7.5.2, 7.5.3, A.5.37
SA-8	Security Engineering Principles	Information System and Services Acquisition Policy	5315 Information Security Integration		9.3.15.6 Security Engineering Principles		A.8.27, A.8.28
SA-9	External Information System Services	Information System and Services Acquisition Policy	5305.8 Provisions for Agreements with State and Non-State Entities 5315.1 System and Services Acquisition	Control 15: Establish and Maintain a Service Provider Management Policy	9.3.15.7 External Information System Services	164.308(b)(1), 164.308(b)(4), 164.314(a)(1), 164.314(a)(2)(i), 164.314(a)(2)(ii)	A.5.2, A.5.4, A.5.8, A.5.14, A.5.22, A.5.23, A.8.21

System Security Risk Management Plan Security Control		SJC Information Security Policy	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	CIS Critical Security Controls (v8)	IRS Publication 1075 Controls	HIPAA Security Controls (45 CFR Parts 164) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
SA-10	Developer Configuration Management	Information System and Services Acquisition Policy	5315.1 System and Services Acquisition 5315.5 Configuration Management	Control 4: Establish and Maintain a Secure Configuration Process	9.3.15.8 Developer Configuration Management		A.8.9, A.8.28, A.8.30, A.8.32
SA-11	Developer Security Testing and Evaluation	Information System and Services Acquisition Policy	5315.1 System and Services Acquisition 5315.4 System Developer Security Testing	Control 16: Implement Code-Level Security Checks	9.3.15.9 Developer Security Testing and Evaluation		A.8.29, A.8.30
System and Communications Protection Family							
SC-1	System and Communications Protection Policy and Procedures	Information System and Communications Protection Policy					5.2, 5.3, 7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2, A.5.4, A.5.31, A.5.36, A.5.37
SC-2	Application Partitioning	Information System and Communications Protection Policy	5350 Operational Security		9.3.16.2 Application Partitioning		None
SC-4	Information In Shared Resources	Information System and Communications Protection Policy	5350 Operational Security	Control 3: Deploy a Data Loss Prevention Solution	9.3.16.3 Information in Shared Resources		None
SC-5	Denial of Service Protection	Information System and Communications Protection Policy	5350 Operational Security		9.3.16.4 Denial of Service Protection		None

System Security Risk Management Plan Security Control		SJC Information Security Policy	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	CIS Critical Security Controls (v8)	IRS Publication 1075 Controls	HIPAA Security Controls (45 CFR Parts 164) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
SC-7	Boundary Protection	<u>Information System and Communications Protection Policy</u>	5350 Operational Security	Control 4: Implement and Manage a Firewall on Servers, Implement and Manage a Firewall on End-User Devices Control 13: Perform Application Layer Filtering	9.3.16.5 Boundary Protection		A.5.14, A.8.16, A.8.20, A.8.22, A.8.23, A.8.26
SC-8	Transmission Confidentiality and Integrity	<u>Information System and Communications Protection Policy</u>	5350 Operational Security 5350.1 Encryption	Control 3: Encrypt Sensitive Data in Transit Control 9 : Restrict Unnecessary or Unauthorized Browser and Email Client Extensions	9.3.16.6 TRANSMISSION CONFIDENTIALITY AND INTEGRITY 4.0 SECURE STORAGE—IRC 6103(P)(4)(B); (4.4 FTI IN TRANSIT) 7.0 REPORTING REQUIREMENTS— 6103(P)(4)(E); (7.1.2 ENCRYPTION REQUIREMENTS)	164.312(C)(1), 164.312(C)(2), 164.312(E)(2)(I) 164.312(E)(2)(II) 164.312(E)(1)	A.5.10, A.5.14, A.8.20, A.8.26
SC-10	Network Disconnect	<u>Information System and Communications Protection Policy</u>	5350 Operational Security		9.3.16.7 Network Disconnect		A.8.20
SC-12	Cryptographic Key Establishment and Management	<u>Information System and Communications Protection Policy</u>	5350 Operational Security 5350.1 Encryption		9.3.16.8 Cryptographic Key Establishment and Management 7.0 Reporting Requirements— 6103(p)(4)(E); (7.1.2 Encryption Requirements)	164.312(e)(2)(ii)	A.8.24

System Security Risk Management Plan Security Control		SJC Information Security Policy	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	CIS Critical Security Controls (v8)	IRS Publication 1075 Controls	HIPAA Security Controls (45 CFR Parts 164) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
SC-13	Cryptographic Protection	<u>Information System and Communications Protection Policy</u>	5350 Operational Security 5350.1 Encryption		9.3.16.9 Cryptographic Protection 7.0 Reporting Requirements—6103(p)(4)(E); (7.1.2 Encryption Requirements)	164.312(a)(2)(iv), 164.312(e)(2)(ii)	A.8.24 A.8.26
SC-15	Collaborative Computing Devices		5350 Operational Security		9.3.16.10 Collaborative Computing Devices		A.5.14
SC-17	Public Key Infrastructure Certificates	<u>Information System and Communications Protection Policy</u>	5350 Operational Security 5350.1 Encryption		9.3.16.11 Public Key Infrastructure Certificates		A.8.24
SC-18	Mobile Code		5350 Operational Security	Control 9: Restrict Unnecessary or Unauthorized Browser and Email Client Extensions	9.3.16.12 Mobile Code		None
SC-20	Secure Name/Address Resolution Service (Authoritative Source)	<u>Information System and Communications Protection Policy</u>	5350 Operational Security				None
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)		5350 Operational Security				None
SC-22	Architecture and Provisioning for Name/Address Resolution Service		5350 Operational Security				None
SC-23	Session Authenticity		5350 Operational Security 5350.1 Encryption	Control 12: Securely Manage Network Infrastructure, Use of Secure Network Management and Communication Protocols	9.3.16.14 Session Authenticity		None

System Security Risk Management Plan Security Control		SJC Information Security Policy	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	CIS Critical Security Controls (v8)	IRS Publication 1075 Controls	HIPAA Security Controls (45 CFR Parts 164) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
SC-28	Protection of Information at Rest		5350 Operational Security 5350.1 Encryption	Control 3: Encrypt Data on End-User Devices, Encrypt Sensitive Data at Rest Control 11: Protect Recovery Data	9.3.16.15 Protection of Information at Rest		A.5.10 A.5.33
SC-39	Process Isolation		5350 Operational Security	Control 4: Separate Enterprise Workspaces on Mobile End-User Devices	9.4.1 Cloud Computing Environments 9.4.11 Storage Area Networks 9.4.14 Virtualization Environments		None
SC-40	Wireless Link Protection		5350 Operational Security		9.4.18 Wireless Networks		None
System and Information Integrity Family							
SI-1	System and Information Integrity Policy and Procedures	<u>Information System Integrity Policy</u>	5350 Operational Security		9.3.17.1 System and Information Integrity Policy and Procedures	164.312(c)(1) 164.316(b)(2)(ii) 164.316(b)(2)(iii)	5.2,5.3,7.5.1, 7.5.2, 7.5.3, A.5.1, A.5.2 A.5.31, A.5.36, A.5.37 A.5.4
SI-2	Flaw Remediation	<u>Information System Integrity Policy</u>	5350 Operational Security	Control 7: Perform Automated Operating System Patch Management, Perform Automated Application Patch Management	9.3.17.2 Flaw Remediation		A.6.8, A.8.3.2 A.8.8
SI-3	Malicious Code Protection	<u>Information System Integrity Policy</u>	5350 Operational Security 5355 Endpoint Defense 5355.1 Malicious Code Protection		9.3.17.3 Malicious Code Protection		A.8.7

System Security Risk Management Plan Security Control		SJC Information Security Policy	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	CIS Critical Security Controls (v8)	IRS Publication 1075 Controls	HIPAA Security Controls (45 CFR Parts 164) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
SI-4	Information System Monitoring	Information System Integrity Policy	5335.1 Continuous Monitoring 5350 Operational Security	Control 13: Centralize Security Event Alerting, deploy a Network Intrusion Detection Solution, Collect Network Traffic Flow Logs, Deploy a Network Intrusion Prevention Solution Control 15: Assess Service Providers	9.3.17.4 Information System Monitoring	164.308(a)(1)(ii)(D)	A.8.16
SI-5	Security Alerts, Advisories and Directives	Information System Integrity Policy					A.5.6 A.8.8
SI-6	Security Function Verification						None
SI-7	Software, Firmware, and Information Integrity	Information System Integrity Policy	5300.5 Minimum Security Controls 5350 Operational Security	Control 2: Allowlist Authorized Scripts Control 12: Establish and Maintain Dedicated Computing Resources for All Administrative Work		164.312(c)(1), 164.312(c)(2), 164.312(e)(2)(i)	None
SI-8	Spam Protection	Information System Integrity Policy	5300.5 Minimum Security Controls 5350 Operational Security	Control 9: Use DNS Filtering Services, Block Unnecessary File Types, Deploy and Maintain Email Server Anti-Malware Protections	9.3.17.6 Spam Protection	164.308(a)(5)(ii)(B)	None
SI-10	Information Input Validation	Information System Integrity Policy	5300.5 Minimum Security Controls 5350 Operational Security		9.3.17.7 Information Input Validation		None
SI-11	Error Handling	Information System Integrity Policy	5300.5 Minimum Security Controls 5350 Operational Security		9.3.17.8 Error Handling		None
SI-12	Information Handling and Retention	Information System Integrity Policy	5300.5 Minimum Security Controls 5350 Operational Security	Control 3, 3.1 Establish and Maintain a Data Management Process	9.3.17.9 Information Handling and Retention	164.316(b)(2)(i)	None
SI-16	Memory Protection		5300.5 Minimum Security Controls 5350 Operational Security	Control 9: Deploy and Maintain Email Server Anti-Malware Protections, Enable Anti-Exploitation Features	9.3.17.10 Memory Protection		None

System Security Risk Management Plan Security Control		SJC Information Security Policy	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	CIS Critical Security Controls (v8)	IRS Publication 1075 Controls	HIPAA Security Controls (45 CFR Parts 164) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
SI-18	Personally Identifiable Information Quality Operations					None	None