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

Departmental Responsibilities
Departments are responsible for reading, understanding, and complying with all Countywide Information Security Policies and ensuring that policies are effectively implemented and communicated to the appropriate users, staff, and management within their area of responsibility.

Management Responsibilities
Individual roles and responsibilities are assigned by County management to ensure accomplishment of Information Security Policy requirements.

Everyone's Responsibility
Many policies are the responsibility of specific individuals, groups or departments in the County; however, there is a subset of policies that are the responsibility of everyone. Anyone with access to County information resources must read, understand and comply with the following Information Security Policies.

County IT Responsibilities
"County IT" refers to all information systems staff, departmental information systems staff, and information systems business units in all San Joaquin County departments, agencies and divisions. "Information Systems Division" specifically refers to the ISD division of the County Administrator's Office.

Policy #:	Title:	Effective Date:
SJC-SEC-POL-1	**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.

1. 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.

2. MAINTENANCE TOOLS
   County IT shall:

   a. Ensure that system owners and County IT approve, control, and monitor information system maintenance tools.

   b. Check media containing diagnostic and test programs for malicious code before the media are used in the information system.

3. 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.

4. 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.

5. 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 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:	12/01/2023

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-2	**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.

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 removeable 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:	12/01/2023

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-3	**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:	12/01/2023

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-4	**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.

      This control applies when reassignments or transfers of individuals are permanent or of such extended durations as to make the actions warranted.

   f. 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:	12/01/2023

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-5	**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.

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:	12/01/2023

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-6	**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:	12/01/2023

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-7	**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, in direct guidance and association with the Department's Information Security Officer shall:

   a. 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.

   b. 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. ACQUISITION PROCESS
   County IT shall:

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

   b. 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 functional requirements.

      ii. Security assurance requirements.

iii. Data sharing or processing agreements where applicable (e.g. HIPAA Business Associate Agreement); and

iv. Acceptance criteria.

3. 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.

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:	12/01/2023

REFERENCE

National Institute of Standards and Technology (NIST) Special Publications (SP): NIST SP 800-53a – System and Services Acquisition (SA), 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;
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-8	**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:	12/01/2023

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-9	**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 that 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.

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:	12/01/2023

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 SP800-83, 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-10	**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 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.

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.

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:	12/01/2023

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-11	**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:	12/01/2023

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-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:	12/01/2023

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	**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:	12/01/2023

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-14	**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.

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. 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).

   c. 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:	12/01/2023

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-15	**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):

   a. 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.

   b. 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.

c. 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.

d. 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.

e. 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:	12/01/2023

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-16	**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.

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, <u>for password-based authentication</u> enforce minimum password complexity for standard user accounts, specifically that passwords meet the following requirements:

      i. Require passwords to have a minimum length of 10 characters;

      ii. Restrict passwords from containing the user's account name, username, or display name;

      iii. Prohibit passwords that are on a list of commonly used passwords per County standards; and

      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; and

   ii. Restrict passwords from containing the user's account name, username, or display name.

   iii. Prohibit passwords that are on a list of commonly used passwords per County standards.

   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 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 shared \ 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. Prohibit password reuse for 5 generations;

l. Allow the use of a temporary password for system logons with an immediate change to a permanent password;

m. 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;

n. Require that the registration process to receive specific authenticators (as password) be conducted in person or by a trusted/vetted third party solution; and

o. Ensure that the information system, for hardware/software token-based authentication complies with County standards.

p. Require that users with multiple identifiers, including staff with separate privileged or administrative accounts, use separate, unique passwords for each of their accounts.

q. At least annually, test the strength of users' passwords stored in Active Directory by attempting to crack the stored hashes. Force the reset of all weak passwords so discovered.

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:	12/01/2023

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-17	**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.

REFERENCE

National Institute of Standards and Technology (NIST) Special Publication (SP): NIST SP 800-53a – Incident Response (IR), NIST SP 800-16, NIST SP 800-50, NIST SP 800-61, NIST SP 800-84, NIST SP 800-115;
State of California State Administrative Manual (SAM) 5300 et seq., Statewide Information Management Manual (SIMM) et seq.

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. Thoroughly document the security incident and related incident response activities.

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. 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.

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:	12/01/2023

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-18	**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:	12/01/2023

REFERENCE

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

Policy #:	Title:	Effective Date:
SJC-SEC-POL-19	**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:	12/01/2023

REFERENCE

Policy #:	Title:	Effective Date:
SJC-SEC-POL-20	**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 7/1/2023, the acting CISO is Mark Thomas, ISD Director.

    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 requesting County Department.

DATE ISSUED/DATE REVIEWED

Date Issued:	12/1/2023
Date Reviewed:	12/1/2023

REFERENCE

Policy #:	Title:	Effective Date:
SJC-SEC-POL-21	**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:	12/01/2023

REFERENCE

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

Policy #:	Title:	Effective Date:
SJC-SEC-POL-22	**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:	12/01/2023

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-23	**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:	12/01/2023

REFERENCE

HITRUST ALLIANCE: https://hitrustalliance.net/
StateRAMP Authorized Product: https://stateramp.org/product-list/
FedRAMP Marketplace: https://marketplace.fedramp.gov/products

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 *Executive Agency*.
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 *Security Control Assessment*.
Assessor	See *Security Control Assessor*.
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 *Authentication*.
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 *Authorization*.
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)]	Agency official responsible for: (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. Note: Organizations subordinate to federal agencies may use the term *Chief Information Officer* to denote individuals filling positions with similar security responsibilities to agency-level Chief Information Officers.
Chief Information Security Officer	See *Senior Agency Information Security Officer*.

Chief Privacy Officer	See *Senior Agency Official for Privacy*.
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 *Security Control Inheritance*.
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.

Defense-in-Breadth [CNSSI 4009]	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).
Defense-in-Depth	Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.
Developer	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.
Digital Media	A form of electronic media where data are stored in digital (as opposed to analog) form.
Discretionary Access Control [CNSSI 4009]	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. 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).
Domain [CNSSI 4009]	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 *Security Domain*.

Enterprise [CNSSI 4009]	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 *Organization*.
Enterprise Architecture [44 U.S.C. Sec. 3601]	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.
Environment of Operation [NIST SP 800-37]	The physical surroundings in which an information system processes, stores, and transmits information.
Event [CNSSI 4009, Adapted]	Any observable occurrence in an information system.
Executive Agency [41 U.S.C., Sec. 403]	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.
Exfiltration	The unauthorized transfer of information from an information system.
External Information System (or Component)	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.
External Information System Service	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.
External Information System Service Provider	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.

External Network	A network not controlled by the organization.
Failover	The capability to switch over automatically (typically without human intervention or warning) to a redundant or standby information system upon the failure or abnormal termination 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 *Executive Agency*.
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 *NSA-Approved Cryptography*.
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 *Software* and *Firmware*.
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 *Common Control* and *System-Specific Security Control*.

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 *Authorization Boundary*.
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.

Information System-Related Security Risks	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 *Risk*.
Information Technology [40 U.S.C., Sec. 1401]	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 *information technology* includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.
Information Technology Product	See *Information System Component*.
Information Type [FIPS 199]	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.
Insider [Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs]	Any person with authorized access to any U.S. Government resource, to include personnel, facilities, information, equipment, networks, or systems.
Insider Threat [Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs]	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.
[CNSSI 4009]	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.

Insider Threat Program [Presidential Memorandum, National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs]	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.
Integrity [44 U.S.C., Sec. 3542]	Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
Internal Network	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.
Label	See *Security Label*.
Line of Business	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.
Local Access	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.
Logical Access Control System [FICAM Roadmap and Implementation Guidance]	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.
Low-Impact System [FIPS 200]	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.

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 *Malicious Code*.
Managed Interface	An interface within an information system that provides boundary protection capability using automated mechanisms or devices.
Mandatory Access Control [CNSSI 4009]	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. 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.
Marking	See *Security Marking*.
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.

Mobile Code Technologies	Software technologies that provide the mechanisms for the production and use of mobile code (e.g., Java, JavaScript, ActiveX, VBScript).
Mobile Device	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.
Moderate-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 moderate and no security objective is assigned a FIPS Publication 199 potential impact value of high.
Multifactor Authentication	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 *Authenticator*.
Multilevel Security [CNSSI 4009]	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.
Multiple Security Levels [CNSSI 4009]	Capability of an information system that is trusted to contain, and maintain separation between, resources (particularly stored data) of different security domains.
National Security Emergency Preparedness Telecommunications Services [47 C.F.R., Part 64, App A]	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.

National Security System [44 U.S.C., Sec. 3542]	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.
Network [CNSSI 4009]	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.
Network Access	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).
Nondiscretionary Access Control	See *Mandatory Access Control*.
Nonlocal Maintenance	Maintenance activities conducted by individuals communicating through a network, either an external network (e.g., the Internet) or an internal network.
Non-Organizational User	A user who is not an organizational user (including public users).
Non-repudiation	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.
NSA-Approved Cryptography	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.
Object	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 *Subject*.

Operations Security [CNSSI 4009]	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.
Organization [FIPS 200, Adapted]	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).
Organizational User	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.
Overlay	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.
Penetration Testing	A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.
Personally Identifiable Information [OMB Memorandum 07-16]	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.).
Physical Access Control System [FICAM Roadmap and Implementation Guidance]	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.
Plan of Action and Milestones [OMB Memorandum 02-01]	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.

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 *limited* adverse effect (FIPS Publication 199 low); (ii) a *serious* adverse effect (FIPS Publication 199 moderate); or (iii) a *severe* or *catastrophic* 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 *Information System Resilience*.

Restricted Data [Atomic Energy Act of 1954]	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].
Risk [FIPS 200, Adapted]	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. 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.
Risk Assessment	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. Part of risk management incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.
Risk Executive (Function) [CNSSI 4009]	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.
Risk Management [CNSSI 4009, adapted]	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.
Risk Mitigation [CNSSI 4009]	Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

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	Actions taken to render data written on media unrecoverable by both ordinary and, for some forms of sanitization, extraordinary means. Process to remove information from media such that data recovery is not possible. It includes removing all classified labels, markings, and activity logs.
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 *Security Control Assessment*.
Security Assessment Plan	The objectives for the security control assessment and a detailed roadmap of how to conduct such an assessment.

Security Assurance	See *Assurance*.
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 *Authorization*.
Security Authorization Boundary	See *Authorization Boundary*.
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 *Security Category*.
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 *Common Control*.
Security Control Overlay	See *Overlay*.
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 *Incident*.
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 *System Security Plan* or *Information Security Program Plan*.

Security Policy [CNSSI 4009]	A set of criteria for the provision of security services.
Security Policy Filter	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.
Security Requirement [FIPS 200, Adapted]	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. 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.
Security Service [CNSSI 4009]	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.
Security-Relevant Information	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.
Senior Agency Information Security Officer [44 U.S.C., Sec. 3544]	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. Note: Organizations subordinate to federal agencies may use the term *Senior Information Security Officer* or *Chief Information Security Officer* to denote individuals filling positions with similar responsibilities to Senior Agency Information Security Officers.
Senior Agency Official for Privacy	The senior organizational official with overall organization-wide responsibility for information privacy issues.

Senior Information Security Officer	See *Senior Agency Information Security Officer*.
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 *Object*.
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 *Information System*.
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 *Tailoring*.
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. See *Organizational User* and *Non-Organizational User*.
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	See *Vulnerability Assessment*.
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: Security and Privacy Control Catalog Compliance Mapping

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	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		5360 Identity and Access Management	Critical Control 15: Controlled Access Based on the Need to Know	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)	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.10.8.1, A.11.1.1, A.11.3.3, A.11.4.1, A.11.6.1, A.11.7.1, A.11.7.2, A.12.3.2, A.15.1.1, A.15.2.1
AC-2	Account Management		5315.8 Information Asset Connections 5335 Information Security Monitoring 5360 Identity and Access Management	"Critical Control 15: Controlled Access Based on the Need to Know	9.3.1.2 Account Management	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.8.3.3, A.11.2.1, A.11.2.2, A.11.2.4, A.11.5.2, A.11.5.5, A.11.5.6
AC-3	Access Enforcement		5350.1 Encryption 5360 Identity and Access Management	"Critical Control 15: Controlled Access Based on the Need to Know	9.3.1.3 Access Enforcement	164.308(a)(3)(ii)(A), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C, 164.310(a)(2)(iii), 164.310(b), 164.312(a)(1), 164.312(a)(2)(i), 164.312(a)(2)(ii), 164.312(a)(2)(iv)	A.7.2.2, A.10.6.1, A.10.7.3, A.10.7.4, A.10.8.1 A.10.9.1, A.10.9.2, A.10.9.3, A.11.2.2, A.11.5.4, A.11.6.1, A.12.4.3, A.15.1.3
AC-4	Information Flow Enforcement		5315.8 Information Asset Connections 5360 Identity and Access Management	Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches. Critical Control 15: Controlled Access Based on the Need to Know. Critical Control 17: Data Loss Prevention	9.3.1.4 Information Flow Enforcement	164.308(a)(3)(ii)(A), 164.308(a)(4)(ii)(B), 164.310(b)	A.7.2.2, A.10.7.3, A.10.8.1, A.11.4.5, A.11.4.7, A.12.5.4

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
AC-5	Separation of Duties		5360 Identity and Access Management		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)(1)	A.10.1.3
AC-6	Least Privilege		5360 Identity and Access Management	Critical Control 12: Controlled Use of Administrative Privileges Critical Control 15: Controlled Access Based on the Need to Know	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)(1)	A.11.2.2, A.11.4.1, A.11.4.4, A.11.5.4, A.11.6.1, A.12.4.3
AC-7	Unsuccessful Logon Attempts		5335 Information Security Monitoring 5335.2 Auditable Events 5360 Identity and Access Management		9.3.1.7 Unsuccessful Logon Attempts		A.11.5.1
AC-8	System Use Notification		5360 Identity and Access Management	9.3.1.8 System Use Notification			A.6.2.2, A.11.5.1, A.15.1.5
AC-11	Session Lock		5360 Identity and Access Management		9.3.1.9 Session Lock	164.310(b), 164.312(a)(2)(iii)	A.11.3.2, A.11.3.3, A.11.5.5
AC-12	Session Termination		5360 Identity and Access Management		9.3.1.10 Session Termination	164.310(b), 164.312(a)(2)(iii)	A.11.5.5
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		5315.8 Information Asset Connections 5360 Identity and Access Management 5360.1 Remote Access	Critical Control 7: Wireless Device Control. Critical Control 12: Controlled Use of Administrative Privileges. Critical Control 13: Boundary Defense. Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs	9.3.1.12 Remote Access 4.0 Secure Storage—IRC 6103(p)(4)(B); (4.7 Telework Locations)	164.310(b)	A.10.6.1, A.10.8.1, A.10.8.5, A.11.4.1, A.11.4.2, A.11.4.6, A.11.7.1, A.11.7.2
AC-18	Wireless Access		5315.8 Information Asset Connections 5360 Identity and Access Management 5360.2 Wireless Access	Critical Control 7: Wireless Device Control	9.3.1.13 Wireless Access		A.10.6.1, A.10.8.1, A.11.4.1, A.11.4.2, A.11.4.6, A.11.7.1

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
AC-19	Access Control for Mobile Devices		5315.8 Information Asset Connections 5360 Identity and Access Management	Critical Control 12: Controlled Use of Administrative Privileges. Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs	9.3.1.14 Access Control for Mobile Devices	164.310(b)	A.9.2.5, A.10.4.1, A.10.7.3, A.11.4.3, A.11.4.6, A.11.7.1
AC-20	Use of External Information Systems		5315.8 Information Asset Connections 5360 Identity and Access Management	Critical Control 13: Boundary Defense	9.3.1.15 Use of External Information Systems		A.6.2.1, A.7.1.3, A.9.2.5, A.10.6.1, A.10.8.1, A.11.4.1, A.11.4.2, A.11.4.6
AC-21	Information Sharing		5315.8 Information Asset Connections 5360 Identity and Access Management		9.3.1.16 Information Sharing Restricting Access—IRC 6103(p)(4)(C); (5.4 Controls over Processing)		None
AC-22	Publicly Accessible Content		5310 Privacy		9.3.1.17 Publicly Accessible Content		A.10.9.3, A.11.6.1
Audit and Accountability Family							
AU-1	Audit and Accountability Policy and Procedures		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)	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1, A.15.3.1
AU-2	Audit Events		5335 Information Security Monitoring 5335.2 Auditable Events	Critical Control 12: Controlled Use of Administrative Privileges. Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs	9.3.3.3 Audit Events 3.0 Record Keeping Requirement (3.2 Electronic and Non-Electronic FTI Logs)	164.308(a)(5)(ii)(C, 164.312(b)	A.10.10.1, A.10.10.2, A.10.10.4, A.10.10.5, A.11.5.4, A.15.3.1
AU-3	Content of Audit Records		5335 Information Security Monitoring 5335.2 Auditable Events	Critical Control 14: Maintenance, Monitoring, and Analysis of Security 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.10.10.1, A.10.10.2, A.10.10.4

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
AU-4	Audit Storage Capacity		5335 Information Security Monitoring 5335.2 Auditable Events	Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs	9.3.3.5 Audit Storage Capacity	164.312(b)	A.10.3.1, A.10.10.3
AU-5	Response to Audit Processing Failures		5335 Information Security Monitoring 5335.2 Auditable Events	Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs	9.3.3.6 Response to Audit Processing Failures	164.312(b)	A.10.3.1, A.10.10.3
AU-6	Audit Review, Analysis, and Reporting		5335 Information Security Monitoring 5335.1 Continuous Monitoring	Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs	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.10.10.2, A.10.10.5, A.13.1.1, A.15.1.5
AU-7	Audit Reduction and Report Generation		5335 Information Security Monitoring 5335.1 Continuous Monitoring		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		5335 Information Security Monitoring 5335.2 Auditable Events	Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs	9.3.3.9 Time Stamps		A.10.10.1, A.10.10.6, A.13.2.3
AU-9	Protection of Audit Information		5335 Information Security Monitoring 5335.2 Auditable Events	Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs	9.3.3.10 Protection of Audit Information		A.10.10.3, A.13.2.3, A.15.1.3, A.15.3.2
AU-11	Audit Record Retention		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.10.10.1, A.13.2.3, A.15.1.3
AU-12	Audit Generation		5335 Information Security Monitoring 5335.2 Auditable Events	Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs	9.3.3.12 Audit Generation		A.10.10.1, A.10.10.2, A.10.10.4, A.10.10.5
Security Assessment and Authorization Family							
CA-3	System Interconnections		5305.8 Provisions for Agreements with State and Non-State Entities	Critical Control 13: Boundary Defense	9.3.4.3 System Interconnections	164.308(b)(1), 164.308(b)(4), 164.314(a)(2)(ii)	A.6.2.1, A.6.2.2, A.6.2.3, A.10.6.1, A.10.6.2, A.10.8.1, A.10.8.2, A.10.8.5, A.11.4.2

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
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)	164.308(a)(1)(ii)(B), 164.308(a)(1)(ii)(C)	None
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)	A.6.1.4, A.10.3.2
CA-7	Continuous Monitoring		5300.5 Minimum Security Controls 5330 Information Security Compliance 5330.1 Security Assessments	Critical Control 20: Penetration Tests and Red Team Exercises	9.3.4.6 Continuous Monitoring	164.308(a)(1)(ii)(D), 164.308(a)(8)	A.6.1.8, A.12.6.1, A.13.1.2, A.15.2.1, A.15.2.2
CA-9	Internal System Connections		5315.8 Information Asset Connections 5360 Identity and Access Management				None
Configuration Management Family							
CM-1	Configuration Management Policy and Procedures		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		A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.12.4.1, A.12.5.1, A.15.1.1, A.15.2.1

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
CM-2	Baseline Configuration		5315.6 Activate only Essential Functionality	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.	9.3.5.2 Baseline Configuration		A.10.1.2, A.10.1.4, A.12.4.1
CM-3	Configuration Change Control		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.	9.3.5.3 Configuration Change Control		A.10.1.2, A.10.3.2, A.12.4.1, A.12.5.1, A.12.5.2, A.12.5.3
CM-4	Security Impact Analysis		5315 Information Security Integration 5315.3 Configuration Management		9.3.5.4 Security Impact Analysis		A.10.1.2, A.10.1.4, A.10.3.2, A.12.4.1, A.12.5.2, A.12.5.3
CM-5	Access Restrictions for Change		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	9.3.5.5 Access Restrictions for Change		A.10.1.2, A.12.4.1, A.12.4.3, A.12.5.3

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
CM-6	Configuration Settings		5315.6 Activate only Essential Functionality	Critical Control 3: Secure Configurations for Hardware and Software. Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches. Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services	9.3.5.6 Configuration Settings		A.10.10.2
CM-7	Least Functionality		5315.6 Activate Only Essential Functionality	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 Critical Control 6: Application Software Security. Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services	9.3.5.7 Least Functionality		A.11.4.1, A.11.4.4, A.11.4.6, A.12.4.1
CM-8	Information System Component Inventory		5305.5 Information Asset Management	Critical Control 1: Inventory of Authorized and Unauthorized Devices Critical Control 2: Inventory of Authorized and Unauthorized Software	9.3.5.8 Information System Component Inventory	164.310(d)(1), 164.310(d)(2)(iii)	A.7.1.1, A.7.1.2
CM-9	Configuration Management Plan		5315.3 Configuration Management	Critical Control 2: Inventory of Authorized and Unauthorized Software	9.3.5.9 Configuration Management Plan		A.6.1.3. A.7.1.1, A.7.1.2, A.10.1.2, A.10.1.4, A.10.3.2, A.12.4.1, A.12.4.3, A.12.5.1, A.12.5.2, A.12.5.3

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
CM-10	Software Usage Restrictions		5315.7 Software Usage Restrictions		9.3.5.10 Software Usage Restrictions		A.12.4.1, A.15.1.2
CM-11	User-Installed Software		5315.7 Software Usage Restrictions		9.3.5.11 User-Installed Software		A.10.4.1, A.10.10.2, A.12.4.1, A.15.1.5
Contingency Planning Family							
CP-2	Contingency Plan		5325 Business Continuity with Technology Recovery		9.3.6.2 Contingency Plan	164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C, 164.308(a)(7)(ii)(E, 164.310(a)(2)(i), 164.312(a)(2)(ii)	A.6.1.2, A.6.1.3, A.9.1.4, A.10.3.1, A.14.1.1, A.14.1.2, A.14.1.3, A.14.1.4, A.14.1.5
CP-3	Contingency Training		5325 Business Continuity with Technology Recovery 5325.2 Technology Recovery Training		9.3.6.3 Contingency Training	164.308(a)(7)(ii)(D)	A.8.2.2
CP-4	Contingency Plan Testing		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.6.1.2, A.14.1.4, A.14.1.5
CP-6	Alternate Storage Site		5305.8 Provisions for Agreements with State and Non-State Entities 5325.4 Alternate Storage and Processing Site		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.9.1.4, A.14.1.3
CP-7	Alternate Processing Site		5325 Business Continuity with Technology Recovery 5325.4 Alternate Storage and Processing Site		9.3.6.6 Alternate Processing Site	164.308(a)(7)(ii)(B), 164.310(a)(2)(i)	A.9.1.4, A.14.1.3

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
CP-8	Telecommunications Services		5305.8 Provisions for Agreements with State and Non-State Entities 5325.5 Telecommunications Services			164.308(a)(7)(ii)(B)	A.9.2.2, A.14.1.3
CP-9	Information System Backup		5325.6 Information System Backups	Critical Control 8: Data Recovery Capability	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.10.5.1, A.14.1.3, A.15.1.3
CP-10	Information System Recovery and Reconstitution		5325 Business Continuity with Technology Recovery 5325.1 Technology Recovery Plan	Critical Control 8: Data Recovery Capability	9.3.6.8 Information System Recovery and Reconstitution	164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C)	A.14.1.3
Identification and Authentication Family							
IA-2	Identification and Authentication (Information Asset Users)		5360 Identity and Access Management	Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches. Critical Control 13: Boundary Defense.	9.3.7.2 Identification and Authentication (Organizational Users)	164.308(a)(5)(ii)(D), 164.312(a)(2)(i), 164.312(d)	A.10.9.1, A.10.9.2, A.11.4.2, A.11.5.1, A.11.5.2
IA-3	Device Identification and Authentication		5360 Identity and Access Management		9.3.7.3 Device Identification and Authentication	164.312(a)(2)(i), 164.312(d)	A.11.4.2, A.11.4.3
IA-4	Identifier Management		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.11.2.1, A.11.5.2
IA-5	Authenticator Management		5350.1 Encryption 5360 Identity and Access Management	Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	9.3.7.5 Authenticator Management Secure Storage—IRC 6103(p)(4)(B) Section 4.0	164.308(a)(5)(ii)(D)	A.11.2.1, A.11.2.3, A.11.3.1, A.11.5.1, A.11.5.2, A.11.5.3
IA-6	Authenticator Feedback		5360 Identity and Access Management		9.3.7.6 Authenticator Feedback	164.308(a)(5)(ii)(D)	A.11.5.1, A.11.5.3

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
IA-7	Cryptographic Module Authentication		5350.1 Encryption 5360 Identity and Access Management	9.3.7.7 Cryptographic Module Authentication (IA-7) 7.0 Reporting Requirements—6103(p)(4)(E); (7.1.2 Encryption Requirements)		164.308(a)(5)(ii)(D)	A.15.1.6
IA-11	Re-authentication		5360 Identity and Access Management				A.11.5.6
Incident Response Family							
IR-1	Incident Response Policy and Procedures		5340 Information Security Incident Management	Critical Control 18: Incident Response Capability	9.3.8.1 Incident Response Policy and Procedures 10.0 Reporting Improper Inspections or Disclosures; (10.1 General)	164.308(a)(6)(i)	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.13.1.1, A.13.2.1, A.15.1.1, A.15.2.1
IR-2	Incident Response Training		5340.1 Incident Response Training	Critical Control 18: Incident Response Capability	9.3.8.2 Incident Response Training	164.308(a)(6)(i)	A.8.2.2, A.10.4.1
IR-3	Incident Response Testing		5340.2 Incident Response Testing		9.3.8.3 Incident Response Testing	164.308(a)(6)(i)	None
IR-4	Incident Handling		5340.3 Incident Handling	Critical Control 18: Incident Response Capability. Critical Control 19: Secure Network Engineering	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.6.1.2, A.6.1.6, A.13.2.1, A.13.2.2, A.13.2.3
IR-5	Incident Monitoring		5340 Information Security Incident Management	Critical Control 18: Incident Response Capability	9.3.8.5 Incident Monitoring	164.308(a)(1)(ii)(D), 164.308(a)(6)(ii)	None

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
IR-6	Incident Reporting		5340.4 Incident Reporting	Critical Control 18: Incident Response Capability	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.6.1.6, A.13.1.1
IR-7	Incident Response Assistance		5340 Information Security Incident Management 5340.3 Incident Handling		9.3.8.7 Incident Response Assistance	164.308(a)(6)(ii)	A.6.1.6
IR-8	Incident Response Plan		5340 Information Security Incident Management 5340.3 Incident Handling		9.3.8.8 Incident Response Plan (IR-8) Reporting Improper Inspections or Disclosures Section 10.0 (10.3)		A.10.4.1
Maintenance Family							
MA-1	System Maintenance Policy and Procedures		5315 Information Security Integration		9.3.9.1 System Maintenance Policy and Procedures	164.310(a)(2)(iv)	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
MA-2	Controlled Maintenance		5315 Information Security Integration		9.3.9.2 Controlled Maintenance	164.310(a)(2)(iv)	A.9.2.4, A.9.2.7, A.11.4.4
MA-3	Maintenance Tools		5315 Information Security Integration		9.3.9.3 Maintenance Tools		A.9.2.4, A.10.4.1
MA-4	Nonlocal Maintenance		5315 Information Security Integration		9.3.9.4 Non-Local Maintenance		A.9.2.4, A.11.4.4
MA-5	Maintenance Personnel		5315 Information Security Integration		9.3.9.5 Maintenance Personnel	164.308(a)(3)(ii)(A)	A.9.1.1, A.9.2.4, A.12.4.3

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
MA-6	Timely Maintenance		5315 Information Security Integration			164.310(a)(2)(iv)	A.9.2.4
Media Protection Family							
MP-1	Media Protection Policy and Procedures		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)	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.10.7.1, A.11.1.1, A.11.3.3, A.12.3.1, A.15.1.1, A.15.1.3, A.15.2.1
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.7.2.2, A.10.7.3, A.11.3.3
MP-3	Media Marking		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.7.2.2, A.10.7.3, A.10.7.4
MP-4	Media Storage		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.10.7.1, A.10.7.4, A.11.3.3, A.15.1.3
MP-5	Media Transport		5350.1 Encryption 5365.2 Media Protection		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.9.2.5, A.9.2.7, A.10.7.1, A.10.8.3
MP-6	Media Sanitization		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.9.2.6, A.10.7.1, A.10.7.2

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
MP-7	Media Use		5365.2 Media Protection				A.10.4.1, A.10.7.1
Physical and Environmental Protection Family							
PE-2	Physical Access Authorizations		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.8.3.3, A.9.1.2
PE-3	Physical Access Control		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.9.1.1, A.9.1.2, A.9.1.3, A.9.1.6, A.11.4.4
PE-4	Access Control for Transmission Medium		5365 Physical Security		9.3.11.4 Access Control for Transmission Medium	164.310(a)(1), 164.310(c	A.9.1.1, A.9.1.2, A.9.1.3, A.9.2.3
PE-5	Access Control for Output Devices		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.9.1.1, A.9.1.2, A.9.1.3
PE-6	Monitoring Physical Access		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.9.1.2, A.10.10.2
PE-8	Visitor Access Records		5335 Information Security Monitoring 5335.1 Continuous Monitoring 5335.2 Auditable Events 5365 Physical Security		9.3.11.7 Visitor Access Records	164.310(a)(2)(iii)	A.9.1.2, A.10.10.2

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
PE-9	Power Equipment and Cabling		5300.5 Minimum Security Controls 5365 Physical Security		Secure Storage—IRC 6103(p)(4)(B); (4.7.1 Equipment)		A.9.1.4, A.9.2.2, A.9.2.3
PE-10	Emergency Shutoff		5300.5 Minimum Security Controls 5365 Physical Security				A.9.2.2
PE-11	Emergency Power		5300.5 Minimum Security Controls 5365 Physical Security				A.9.2.2
PE-12	Emergency Lighting		5300.5 Minimum Security Controls 5365 Physical Security				A.9.2.2
PE-13	Fire Protection		5300.5 Minimum Security Controls 5365 Physical Security				A.6.1.6, A.9.1.4, A.9.2.1
PE-14	Temperature and Humidity Controls		5300.5 Minimum Security Controls 5335.1 Continuous Monitoring 5365 Physical Security				A.9.2.1, A.9.2.2
PE-15	Water Damage Protection		5300.5 Minimum Security Controls 5335.1 Continuous Monitoring 5365 Physical Security				A.9.1.4, A.9.2.1
PE-16	Delivery and Removal		5365 Physical Security		9.3.11.8 Delivery and Removal		A.9.1.6, A.9.2.7
PE-17	Alternate Work Site		5365 Physical Security		9.3.11.9 Alternate Work Site	164.310(a)(2)(i)	A.9.2.5, A.11.7.2
PE-19	Information Leakage		5365 Physical Security				A.9.1.4, A.9.2.1, A.12.5.4
Planning Family							

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
PL-4	Rules of Behavior		5305.8 Provisions for Agreements with State and Non-State Entities		9.3.12.3 Rules of Behavior		A.6.1.5, A.6.2.2, A.6.2.3, A.7.1.3. A.8.1.1, A.8.1.3, A.8.2.1, A.10.8.1, A.11.7.1, A.11.7.2, A.13.1.2, A.15.1.5
PL-8	Information Security Architecture		5315 Information Security Integration				A.12.1.1
Personnel Security							
PS-4	Personnel Termination		5305.4 Personnel Management		9.3.13.4 Termination	164.308(a)(3)(ii)(C)	A.8.3.1, A.8.3.2, A.8.3.3
PS-5	Personnel Transfer		5305.4 Personnel Management		9.3.13.5 Personnel Transfer	164.308(a)(3)(ii)(C)	A.8.3.1, A.8.3.2, A.8.3.3
PS-6	Access Agreements		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.6.1.5, A.6.2.3, A.7.1.3, A.8.1.1, A.8.1.3, A.8.2.1, A.10.8.1, A.11.7.1, A.11.7.2, A.15.1.5
Risk Assessment Family							

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
RA-5	Vulnerability Scanning		5330.1 Security Assessments 5335 Information Security Monitoring 5335.1 Continuous Monitoring 5345 Vulnerability and Threat Management	Critical Control 4: Continuous Vulnerability Assessment and Remediation. Critical Control 6: Application Software Security. Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches. Critical Control 13: Boundary Defense. Critical Control 20: Penetration Tests and Red Team Exercises.	9.3.14.3 Vulnerability Scanning		A.12.6.1, A.15.2.2
System and Services Acquisition Family							
SA-3	System Development Life Cycle		5315 Information Security Integration 5315.2 System Development Lifecycle	Critical Control 6: Application Software Security	9.3.15.3 System Development Life Cycle		A.6.1.3, A.12.1.1
SA-4	Acquisition Process		5305.8 Provisions for Agreements with State and Non-State Entities 5315 Information Security Integration 5315.1 System and Services Acquisition	Critical Control 3: Secure Configurations for Hardware and Software. Critical Control 6: Application Software Security.	9.3.15.4 Acquisition Process	164.314(a)(2)(i)	A.10.3.2, A.12.1.1, A.12.5.5
SA-5	Information System Documentation		5315 Information Security Integration 5315.3 Information Asset Documentation		9.3.15.5 Information System Documentation		A.10.1.1, A.10.7.4, A.13.1.2, A.15.1.3
SA-8	Security Engineering Principles		5315 Information Security Integration	Critical Control 6: Application Software Security. Critical Control 19: Secure Network Engineering.	9.3.15.6 Security Engineering Principles		A.10.4.2, A.12.1.1

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
SA-9	External Information System Services		5305.8 Provisions for Agreements with State and Non-State Entities 5315.1 System and Services Acquisition		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.6.1.3, A.6.1.5, A.6.2.1, A.6.2.2, A.6.2.3, A.8.2.1, A.10.2.1, A.10.2.2, A.10.2.3, A.10.6.2, A.10.8.2, A.12.5.5
SA-10	Developer Configuration Management		5315.1 System and Services Acquisition 5315.5 Configuration Management		9.3.15.8 Developer Configuration Management		A.10.1.2, A.10.1.4, A.10.2.3, A.10.3.2, A.12.4.3, A.12.5.1, A.12.5.3, A.12.5.5
SA-11	Developer Security Testing and Evaluation		5315.1 System and Services Acquisition 5315.4 System Developer Security Testing		9.3.15.9 Developer Security Testing and Evaluation		A.6.1.8, A.10.3.2, A.12.5.5, A.13.1.2
System and Communications Protection Family							
SC-2	Application Partitioning		5350 Operational Security		9.3.16.2 Application Partitioning		A.10.4.2, A.10.9.2, A.11.4.5, A.11.5.4
SC-4	Information In Shared Resources		5350 Operational Security		9.3.16.3 Information in Shared Resources		None
SC-5	Denial of Service Protection		5350 Operational Security		9.3.16.4 Denial of Service Protection		A.10.3.1, A.10.6.1
SC-7	Boundary Protection		5350 Operational Security	Critical Control 10: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches. Critical Control 11: Limitation and Control of Network Ports, Protocols, and Services. Critical Control 13: Boundary Defense.	9.3.16.5 Boundary Protection		A.10.4.1, A.10.4.2, A.10.6.1, A.10.8.1, A.10.8.4, A.10.9.1, A.10.9.2, A.10.10.2, A.11.4.1, A.11.4.5, A.11.4.6, A.11.4.7, A.11.6.2

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
SC-8	Transmission Confidentiality and Integrity		5350 Operational Security 5350.1 Encryption		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)	A.10.6.1, A.10.8.1, A.10.8.4, A.10.9.1, A.10.9.2, A.12.2.3
SC-10	Network Disconnect		5350 Operational Security		9.3.16.7 Network Disconnect		A.10.6.1, A.11.3.2, A.11.5.5
SC-12	Cryptographic Key Establishment and Management		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.12.3.2
SC-13	Cryptographic Protection		5350 Operational Security 5350.1 Encryption	Critical Control 17: Data Loss Prevention	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.10.9.1, A.10.9.2, A.15.1.6
SC-15	Collaborative Computing Devices		5350 Operational Security		9.3.16.10 Collaborative Computing Devices		A.10.8.1
SC-17	Public Key Infrastructure Certificates		5350 Operational Security 5350.1 Encryption		9.3.16.11 Public Key Infrastructure Certificates		A.12.3.2
SC-18	Mobile Code		5350 Operational Security	Critical Control 5: Malware Defenses. Critical Control 13: Boundary Defense	9.3.16.12 Mobile Code		A.10.4.2, A.12.4.1

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
SC-19	Voice Over Internet Protocol		5350 Operational Security		9.3.16.13 Voice over Internet Protocol 9.4.15 VoIP Systems		None
SC-20	Secure Name/Address Resolution Service (Authoritative Source)		5350 Operational Security	Critical Control 19: Secure Network Engineering			A.10.6.1
SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)		5350 Operational Security	Critical Control 19: Secure Network Engineering			A.10.6.1
SC-22	Architecture and Provisioning for Name/Address Resolution Service		5350 Operational Security	Critical Control 19: Secure Network Engineering			A.10.6.1
SC-23	Session Authenticity		5350 Operational Security 5350.1 Encryption		9.3.16.14 Session Authenticity		None
SC-28	Protection of Information at Rest		5350 Operational Security 5350.1 Encryption	Critical Control 17: Data Loss Prevention	9.3.16.15 Protection of Information at Rest		None
SC-39	Process Isolation		5350 Operational Security		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		5350 Operational Security		9.3.17.1 System and Information Integrity Policy and Procedures	164.312(c)(1)	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.2, A.6.1.3, A.8.1.1, A.10.1.1, A.10.4.1, A.15.1.1, A.15.2.1
SI-2	Flaw Remediation		5350 Operational Security		9.3.17.2 Flaw Remediation		A.12.6.1, A.13.1.2

System Security Risk Management Plan Security Control			California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	SANS 20 (*Twenty Critical Controls*)	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	ISO/IEC 27001 Controls
SI-3	Malicious Code Protection		5350 Operational Security 5355 Endpoint Defense 5355.1 Malicious Code Protection	Critical Control 5: Malware Defenses Critical Control 6: Application Software Security	9.3.17.3 Malicious Code Protection	164.308(a)(5)(ii)(B)	A.10.4.1, A.10.9.3
SI-4	Information System Monitoring		5335.1 Continuous Monitoring 5350 Operational Security	Critical Control 7: Wireless Device Control. Critical Control 13: Boundary Defense. Critical Control 14: Maintenance, Monitoring, and Analysis of Security Audit Logs. Critical Control 17: Data Loss Prevention.	9.3.17.4 Information System Monitoring	164.308(a)(1)(ii)(D), 164.308(a)(5)(ii)(B)	A.10.9.3, A.10.10.2, A.10.10.3, A.15.3.1
SI-7	Software, Firmware, and Information Integrity		5300.5 Minimum Security Controls 5350 Operational Security	Critical Control 3: Secure Configurations for Hardware and Software		164.312(c)(1), 164.312(c)(2), 164.312(e)(2)(i)	A.10.4.1, A.10.9.3, A.10.10.2, A.12.2.2, A.12.2.3, A.12.4.1
SI-8	Spam Protection		5300.5 Minimum Security Controls 5350 Operational Security		9.3.17.6 Spam Protection	164.308(a)(5)(ii)(B)	None
SI-10	Information Input Validation		5300.5 Minimum Security Controls 5350 Operational Security	Critical Control 6: Application Software Security	9.3.17.7 Information Input Validation		A.10.7.3, A.10.9.3, A.12.2.1, A.12.2.2
SI-11	Error Handling		5300.5 Minimum Security Controls 5350 Operational Security		9.3.17.8 Error Handling		None
SI-12	Information Handling and Retention		5300.5 Minimum Security Controls 5350 Operational Security		9.3.17.9 Information Handling and Retention		A.10.7.3, A.15.1.3, A.15.1.4
SI-16	Memory Protection		5300.5 Minimum Security Controls 5350 Operational Security		9.3.17.10 Memory Protection		None

System Security Plan Privacy Control		SCO Information Security Program Standard(s)	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	Information Practices Act of 1977 (State) *(California Civil Code, Title 1.8 Personal Data, Chapter 1 [§1798-1798.78])*	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	The Privacy Act of 1974 (Federal)
AP-1	Authority and Purpose	500 Privacy Standards	5310 Privacy	1798.14, 1798.24, 1798.30			5 U.S.C. § 552a (e)
AP-2	Purpose Specification	500 Privacy Standards	5310 Privacy	1798.17, 1798.24, 1798.30, 1798.60			5 U.S.C. § 552a (e)(3)(A)-(B)
AR-3	Privacy Requirements for Contractors and Service Providers	500 Privacy Standards	5310 Privacy 5310.3 Limiting Use and Disclosure 5310.7 Security Safeguards	1798.19, 1798.20, 1798.21, 1798.24		164.308(b)(1), 164.308(b)(4), 164.314(a)(1), 164.314(a)(2)(i), 164.314(a)(2)(ii)	5 U.S.C. § 552a(m)
AR-4	Privacy Monitoring and Auditing	122 Risk Assessment 130 Security Compliance 203 Project System Security Plans 101 User Activity Monitoring Notice 406 Audit Trails	5310 Privacy 5310.3 Limiting Use and Disclosure	1798.22	Other Safeguards—IRC 6103(p)(4)(D) Section 6.0	164.312(b), 164.308(a)(1)(ii)(D)	5 U.S.C. § 552a
AR-7	Privacy-Enhanced System Design and Development	122 Risk Assessment 130 Security Compliance 203 Project System Security Plans	5305.8 Provisions for Agreements with State and Non-State Entities 5310 Privacy 5310.3 Limiting Use and Disclosure 5310.7 Security Safeguards	1798.20, 1798.21			5 U.S.C. § 552a(e)(10)
AR-8	Accounting for Disclosures	101-User Access Monitoring Notice 406 Audit Trails 500 Privacy Standards	5310 Privacy 5310.3 Limiting Use and Disclosure 5310.7 Security Safeguards	1798.25, 1798.27		164.312(b), 164.308(a)(1)(ii)(D)	5 U.S.C. § 552a (c)(1), (c)(3), (j), (k)

System Security Plan Privacy Control		SCO Information Security Program Standard(s)	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	Information Practices Act of 1977 (State) *(California Civil Code, Title 1.8 Personal Data, Chapter 1 [§1798-1798.78])*	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	The Privacy Act of 1974 (Federal)
DI-1	Data Quality	500 Privacy Standards	5310 Privacy 5310.5 Information Integrity 5310.7 Security Safeguards	1798.15, 1798.16, 1798.18		164.312(e)(2)(i), 164.312(c)(2)	5 U.S.C. § 552a (c) and (e)
DM-1	Minimization of Personally Identifiable Information	122 Risk Assessment 130 Security Compliance 500 Privacy Standards	5310 Privacy 5310.2 Limiting Collection	1798.24			5 U.S.C. §552a (e)
DM-2	Data Retention and Disposal	122 Risk Assessment 130 Security Compliance 500 Privacy Standards	5310 Privacy 5310.5 Information Integrity 5310.6 Data Retention and Destruction 5310.7 Security Safeguards	1798.18, 1798.27, 1798.64			5 U.S.C. § 552a (e)(1), (c)(2)
DM-3	Minimization of PII Used in Testing, Training, and Research	122 Risk Assessment 130 Security Compliance 500 Privacy Standards	5310 Privacy 5310.7 Security Safeguards	1798.21			
SE-1	Inventory of Personally Identifiable Information	207 System Inventory	5305.5 Information Asset Management 5310 Privacy 5310.6 Data Retention and Destruction 5310.7 Security Safeguards	1798.18, 1798.21		164.310(d)(1), 164.310(d)(2)(iii)	5 U.S.C. § 552a (e) (10)

System Security Plan Privacy Control		SCO Information Security Program Standard(s)	California State Administrative Manual (SAM) Section 5300 & State Information Management Manual (SIMM) Sections	Information Practices Act of 1977 (State) *(California Civil Code, Title 1.8 Personal Data, Chapter 1 [§1798-1798.78])*	IRS Publication 1075 Controls	HIPAA Security Controls (*45 CFR Parts 164*) (Ref. NIST SP 800-66)	The Privacy Act of 1974 (Federal)
SE-2	Privacy Incident Response	122 Risk Assessment 130 Security Compliance 203 Project System Security Plans 317 Information Security Incident Reporting SCO Information Memorandum 07-07	5310 Privacy 5310.7 Security Safeguards	1798.21, 1798.29		164.308(a)(6)(i), 164.308(a)(6)(ii)	5 U.S.C. § 552a (e), (i)(1), and (m)
TR-1	Privacy Notice	500 Privacy Standards	5310 Privacy 5310.1 State Entity Privacy Statement and Notice on Collection 5310.5 Information Integrity SIMM 5310-A	1798.17, 1798.32 California Government Code § 11019.9			5 U.S.C. § 552a (e)(3), (e)(4)
UL-1	Internal Use	122 Risk Assessment 203 Project System Security Plans 500 Privacy Standards	5310 Privacy 5310.3 Limiting Use and Disclosure 5310.7 Security Safeguards	1798.17, 1798.24		164.308(a)(3)(ii)(A), 164.308(a)(3)(ii)(B), 164.308(a)(1)(ii)(D)	5 U.S.C. § 552a (b)(1)
UL-2	Information Sharing with Third Parties	500 Privacy Standards	5305.8 Provisions for Agreements with State and Non-State Entities 5310 Privacy 5310.3 Limiting Use and Disclosure 5310.7 Security Safeguards	1798.17, 1798.20, 1798.21, 1798.24		164.308(b)(1), 164.308(b)(4), 164.314(a)(1), 164.314(a)(2)(i), 164.314(a)(2)(ii)	5 U.S.C. § 552a (a)(7), (b), (c), (e)(3)(C), (o)