County of Orange

Cost Reduction Program

AMENDMENT THREE - PARTICIPATING AMENDMENT

THIS THIRD AMENDMENT, to Agreement Number AMR0121, entered into on July 1, 2021, as amended on May 23, 2024 and February 6, 2025 (hereinafter "Participating Amendment") is made and entered into upon execution of all necessary signatures, between the **County of Orange**, a political subdivision of the State of California (hereinafter "County") and **Public Consulting Group LLC,** a Delaware limited liability company, qualified to transact interstate business in the State of California, (hereinafter "CONTRACTOR"), which are sometimes individually referred to as "Party", or collectively referred to as "Parties".

WHEREAS, County of Orange has implemented the Contract Cost Reduction Program to reduce contract costs by ten percent in exchange for one year contract extension or fifteen percent for two years contract extension; and

WHEREAS, County and CONTRACTOR entered into Agreement AMR0121 for SUPPLEMENTAL SECURITY INCOME (SSI), STATE SUPPLEMENTARY PAYMENTS (SSP), AND SOCIAL SECURITY DISABILITY INSURANCE (SSDI) CLIENT ADVOCACY SERVICES; MA-063-21011844 commencing on July 1, 2021, and expiring on June 30, 2026, (hereinafter referred to as "Agreement"); and

WHEREAS, CONTRACTOR has voluntarily agreed to participate in the program by execution of this Participating Amendment; and

WHEREAS, Orange County Board of Supervisors has approved staff's implementation of a Contract Cost Reduction Program to extend existing contracts in exchange for a reduction in costs to the County; and

NOW, THEREFORE, in consideration of the mutual obligations set forth herein, both County and CONTRACTOR agree to amend the Contract as follows:

1. Orange County Contract Cost Reduction Program – Selection:

CONTRACTOR shall choose either Option 1 or Option 2 to participate in the Orange County Contract Cost Reduction Program.

☒ Option 1: A 10% discount for a one-year extension beyond the current contract expiration date;

or

☐ Option 2: A 15% discount for a two-year extension beyond the current contract expiration date.

Subordinate agreements created against this Regional Cooperative Agreement post execution of this Participating Amendment shall receive the same reduction as the Option selected herein.

2. Orange County Contract Cost Reduction Program – Term:

The term of this Participating Amendment shall commence upon execution of all necessary signatures and continue in full force and effect until June 30, 2027, the expiration date corresponding to the option selected by the CONTRACTOR above.

3. Agreement Increase Amount:

Agreement Increase in a total amount of $297,000. annually through the extended term, totaling a revised Not-To-Exceed Amount of: $1,641,000.

4. Orange County Contract Cost Reduction Program – Invoicing Procedures:

During the term of this Participating Amendment, the CONTRACTOR shall include the applicable discount percentage on each invoice submitted to the County for payment. Each invoice shall include the current Agreement pricing minus the discounted price. The applicable percentage discount shall be included in all invoices for services performed, or goods provided, on and after the date of execution of this Participating Amendment through the expiration date corresponding to the option selected by the CONTRACTOR above.

5. Orange County Contract Cost Reduction Program – No Compete Contract Extension:

Participating CONTRACTORS will be granted an extension beyond the current agreement term under the following conditions: (i) the County department has an ongoing need to purchase the products and services and market analysis is favorable to support the extension; (ii) the contract extension period is approved by the department; (iii) the County department has the appropriate fiscal appropriations for each year during the term of the extension, and if such appropriations are not approved by the County Board of Supervisors, the contract will be terminated without penalty to the County; and (iv) the CONTRACTOR's past performance and quality of goods and services has remained satisfactory and at the levels required by the original contract.

6. Subparagraph 4.2 of Exhibit A of the Agreement is hereby amended to read as follows:

4.2 CONTRACTOR's holiday schedule shall not exceed COUNTY's holiday schedule which is as follows: New Year's Day, Martin Luther King Jr. Day, President Lincoln's Birthday, Presidents' Day, Memorial Day, Independence Day, Labor Day, Native American Day, Veterans Day, Thanksgiving Day, Friday after Thanksgiving Day, and Christmas Day. CONTRACTOR shall obtain prior written approval from ADMINISTRATOR for any closure outside of COUNTY's holiday schedule and the hours listed in Subparagraph 4.1 of this Exhibit A. Any unauthorized closure shall be deemed a material breach of this Contract, pursuant to Paragraph 20, and shall not be reimbursed.

7. **Subparagraph 5.9.4 of Exhibit A of the Agreement is hereby amended to read as follows:**

5.9.4 Be responsible to provide all necessary equipment for its staff.

8. **Subparagraph 7.7 of Exhibit A of the Agreement is hereby removed in its entirety.**

9. **Paragraph 14 of the Agreement is hereby amended to read as follows:**

14. INSURANCE

A. Prior to the provision of services under this Agreement, CONTRACTOR agrees to carry all required insurance at Contractor's expense, including all endorsements required herein, necessary to satisfy County that the insurance provisions of this Agreement have been complied with. CONTRACTOR agrees to keep such insurance coverage current and provide Certificates of Insurance and endorsements to County during the entire term of this Agreement.

B. CONTRACTOR shall ensure that all subcontractors performing work on behalf of CONTRACTOR pursuant to this Agreement shall be covered under CONTRACTOR's insurance as an Additional Insured or maintain insurance subject to the same terms and conditions as set forth herein for CONTRACTOR. CONTRACTOR shall not allow subcontractors to work if subcontractors have less than the level of coverage required by County from CONTRACTOR under this Agreement. It is the obligation of CONTRACTOR to provide notice of the insurance requirements to every subcontractor and to receive proof of insurance prior to allowing any subcontractor to begin work. Such proof of insurance must be maintained by CONTRACTOR through the entirety of this Agreement for inspection by County representative(s) at any reasonable time.

C. All self-insured retentions (SIRs) shall be clearly stated on the Certificate of Insurance. Any SIRs in excess of $50,000 shall specifically be approved by the County's Risk Manager, or designee. County reserves the right to require current audited financial reports from CONTRACTOR. If CONTRACTOR is self-insured, CONTRACTOR will indemnify County for any and all claims resulting or arising from CONTRACTOR's services in accordance with the indemnity provision stated in this Agreement.

D. If CONTRACTOR fails to maintain insurance acceptable to County for the full term of this Contract, County may terminate this Agreement.

E. Qualified Insurer

1. The policy or policies of insurance must be issued by an insurer with a minimum rating of A- (Secure A.M. Best's Rating) and VIII (Financial Size Category as determined by the most current edition of the Best's Key Rating Guide/Property-Casualty/United States or ambest.com).

2. If the insurance carrier does not have an A.M. Best Rating of A-/VIII, the CEO/Office of Risk Management retains the right to approve or reject a carrier after a review of the company's performance and financial ratings.

3. The policy or policies of insurance maintained by CONTRACTOR shall provide the minimum limits and coverage as set forth below.

4. Increased insurance limits may be satisfied with Excess/Umbrella policies. Excess/Umbrella policies when required must provide Follow Form coverage.

F. Required Coverage Forms

1. Commercial General Liability coverage shall be written on occurrence basis utilizing Insurance Services Office (ISO) form CG 00 01, or a substitute form providing liability coverage at least as broad.

2. Business Auto Liability coverage shall be written on ISO form CA 00 01, CA 00 05, CA 0012, CA 00 20, or a substitute form providing coverage at least as broad.

G. Required Endorsements

1. Commercial General Liability policy shall contain the following endorsements, which shall accompany the Certificate of Insurance:

a. An Additional Insured endorsement using ISO form CG 20 26 04 13, or a form at least as broad, naming the County of Orange, its elected and appointed officials, officers, employees, and agents as Additional Insureds or provide blanket coverage, which will state AS REQUIRED BY WRITTEN CONTRACT.

b. A primary non-contributory endorsement using ISO form CG 20 01 04 13, or a form at least as broad, evidencing that CONTRACTOR's insurance is primary and any insurance or self-insurance maintained by the County shall be excess and non-contributory.

2. The Workers' Compensation policy shall contain a waiver of subrogation endorsement waiving all rights of subrogation against the County of Orange, its elected and appointed officials, officers, employees, and agents or provide blanket coverage, which will state AS REQUIRED BY WRITTEN CONTRACT.

3. The Network Security and Privacy Liability policy shall contain the following endorsements which shall accompany the Certificate of Insurance.

a. An Additional Insured endorsement naming the County of Orange, its elected and appointed officials, officers, employees, and agents as Additional Insureds for its vicarious liability.

b. A primary and non-contributory endorsement evidencing that the CONTRACTOR's insurance is primary, and any insurance or self-insurance maintained by the County shall be excess and non-contributing.

H. All insurance policies required by this Agreement shall waive all rights of subrogation against the County of Orange, its elected and appointed officials, officers, employees, and agents when acting within the scope of their appointment or employment.

I. CONTRACTOR shall provide 30 days prior written notice to the County of any policy cancellation or non-renewal and 10 days prior written notice where cancellation is due to non-payment of premium and provide a copy of the cancellation notice to County. Failure

to provide written notice of cancellation may constitute a material breach of the Agreement, upon which the County may suspend or terminate this Agreement.

J. If CONTRACTOR's Network Security & Privacy Liability and/or Sexual Misconduct Liability policy is a "Claims-Made" policy(ies), CONTRACTOR shall agree to the following:

1. The retroactive date must be shown and must be before the date of the Agreement or the beginning of the Agreement services.
2. Insurance must be maintained, and evidence of insurance must be provided for at least three (3) years for Network Security & Privacy Liability or (5) years for Sexual Misconduct Liability after expiration or earlier termination of Contract services.
3. If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a retroactive date prior to the effective date of the Contract services, CONTRACTOR must purchase an extended reporting period for a minimum of three years after expiration of earlier termination of the Agreement.

K. The Commercial General Liability policy shall contain a severability of interests clause also known as a "separation of insureds" clause (standard in the ISO CG 0001 policy).

L. Insurance certificates should be forwarded to County at the address indicated in Paragraph 11 of this Agreement.

M. If CONTRACTOR fails to provide the insurance certificates and endorsements within seven days of notification by CEO/County Procurement Office or Deputy Procurement Agent, award may be made to the next qualified proponent.

N. County expressly retains the right to require CONTRACTOR to increase or decrease insurance of any of the above insurance types throughout the term of this Agreement. Any increase or decrease in insurance will be as deemed by County of Orange Risk Manager as appropriate to adequately protect County.

O. County shall notify CONTRACTOR in writing of changes in the insurance requirements. If CONTRACTOR does not provide acceptable Certificates of Insurance and endorsements to County incorporating such changes within 30 days of receipt of such notice, this Agreement may be in breach without further notice to CONTRACTOR, and County shall be entitled to all legal remedies.

P. The procuring of such required policy or policies of insurance shall not be construed to limit CONTRACTOR's liability hereunder nor to fulfill the indemnification provisions and requirements of this Contract, nor act in any way to reduce the policy coverage and limits available from the insurer.

COVERAGE	MINIMUM LIMITS
Commercial General Liability	$1,000,000 per occurrence $2,000,000 aggregate

Automobile Liability including coverage for owned or scheduled, non-owned, and hired vehicles	$1,000,000 combined single limit each accident
Workers' Compensation	Statutory
Employer's Liability Insurance	$1,000,000 per accident or disease
Network Security and Privacy Liability	$1,000,000 per claims-made
Sexual Misconduct Liability	$1,000,000 per occurrence

10. Subparagraph 19.1 of the Agreement is hereby amended to read as follows:

19.1 Use of COUNTY Computer Equipment

County intends to permit CONTRACTOR the use of computer equipment provided by County. Said computer equipment shall be used solely by employees of CONTRACTOR, for the purpose of, and while performing their assigned duties pursuant to this Agreement, and shall remain the property of County. CONTRACTOR shall ensure that each of its employees, volunteers, consultants, or agents that have access to County facilities and/or data completes information security and computer usage training provided by County, signs and adheres to the provisions as they currently exist and as they may be hereafter amended in Attachments A, B, and C to this Agreement and signs and adheres to any subsequent contracts required by federal or State laws or regulations. CONTRACTOR's failure to have all CONTRACTOR employees that have access to County's facilities and/or data execute the contracts and/or complete the training shall constitute a breach of this Agreement.

11. Paragraph 31 of the Agreement is hereby amended to read as follows:

31. SECURITY

CONTRACTOR shall abide by the requirements in Attachment A – Information Technology Security Provisions, Attachment B – OCSSA State Privacy and Security Provisions, and Attachment C – Information Technology Security Guidelines.

12. Attachments

Attachments A, B, and C of the Agreement are hereby replaced in their entirety and are attached as follows. Attachment D of the Agreement is hereby removed in its entirety.

13. All other terms and conditions

All other terms and conditions of the original Contract and any subsequent amendments, unless specifically modified by this Participating Amendment, are hereby incorporated by reference as if fully stated herein and shall remain in full force and effect.

SIGNATURE PAGE

IN WITNESS WHEREOF, the Parties hereto have executed this Contract on the date following their respective signatures.

If the Contractor is a corporation, signatures of two specific corporate officers are required as further set forth.

- The first corporate officer signature must be one of the following: 1) Chairman of the Board, 2) President, 3) Vice President; and
- The second corporate officer signature must be one of the following: 1) Secretary, 2) Assistant Secretary, 3) Chief Financial Officer, 4) Assistant Treasurer.

In the alternative, a single corporate signature is acceptable when accompanied by a corporate resolution demonstrating the legal authority of the signature to bind the company.

Public Consulting Group LLC

Signature	Name	Title	Date
Signed by: Kathy Fallon 87C4B90B973E4F8...	Kathy Fallon	Practice area director	3/5/2026 | 3:25:55 PM PST
Signature	Name	Title	Date

COUNTY OF ORANGE, a political subdivision of the State of California

COUNTY AUTHORIZED SIGNATURE:

Signature	Name	Title	Date
		Deputy Procurement Agent	

Approved as to form:
County Counsel

Signature	Name	Title	Date
Signed by: Mark Batarse 2C0D431...	Mark Batarse	**Deputy**	3/6/2026 | 11:24:21 AM PST

ATTACHMENT A - INFORMATION TECHNOLOGY SECURITY PROVISIONS

1. Contractor's Policies, Procedures, and Technical, Physical, and Administrative Safeguards:

All Contractors with access to County data and/or systems shall establish and maintain policies, procedures, and technical, physical, and administrative safeguards designed to:

A. Ensure the confidentiality, integrity, and availability of all County data and any other confidential information that the Contractor receives, stores, maintains, processes, transmits, or otherwise accesses in connection with the provision of the contracted services,

B. Protect against any threats or hazards to the security or integrity of County data, systems, or other confidential information,

C. Protect against unauthorized access, use, or disclosure of personal or County confidential information,

D. Maintain reasonable procedures to prevent, detect, respond, and provide notification to the County regarding any internal or external security breaches,

E. Ensure the return or appropriate disposal of personal information or other confidential information upon contract conclusion (or per retention standards set forth in the contract), and

F. Ensure that any subcontractor(s)/agent(s) that receives, stores, maintains, processes, transmits, or otherwise accesses County data and/or system(s) is in compliance with statements and the provisions of statements and services herein.

2. County of Orange Information Technology Security Provisions Document:

This County of Orange Information Technology Security Provisions document provides a high-level guide for contractors to understand the resiliency and cybersecurity expectations of the County. The County of Orange Security Guidelines follow the latest National Institute of Standards and Technology (NIST) 800-53 framework to ensure the highest levels of operational resiliency and cybersecurity.

Contractor, Contractor personnel, Contractor's subcontractors, any person performing work on behalf of Contractor, and all other agents and representatives of Contractor will, at all times, comply with and abide by all County of Orange Information Technology Security Provisions ("Security Provisions") that pertain to Contractor(s) in connection with the Services performed by Contractor(s) as set forth in the scope of work of this Contract. Any violations of the Security Provisions shall, in addition to all other available rights and remedies available to County, be cause for immediate termination of this Contract. Such Security Provisions include, but are not limited to, County of Orange Information Technology Security Guidelines, as applicable, and Business Associate Agreement.

Contractor shall use industry best practices and methods with regard to confidentiality, integrity, availability, and the prevention, detection, response, and elimination of threat, by all appropriate means, of fraud, abuse, and other inappropriate or unauthorized access to County data and/or system(s) accessed in the performance of Services under this Contract.

3. **Contractor's Information Security Program:**

The Contractor shall implement and maintain a written information security program that contains reasonable and appropriate security measures designed to safeguard the confidentiality, integrity, availability, and resiliency of County data and/or system(s). The Contractor shall review and update its information security program in accordance with contractual, legal, and regulatory requirements. Contractor shall provide to County a copy of the organization's information security program and/or policies.

4. **Information Access:**

A. Contractor shall use appropriate safeguards and security measures to ensure the confidentiality and security of all County data. County may require all Contractor personnel, subcontractors, and affiliates approved by County to perform work under this Contract to execute a confidentiality and non-disclosure agreement concerning access protection and data security in the form provided by County. County shall authorize, and Contractor shall issue, any necessary information-access mechanisms, including access IDs and passwords, and in no event shall Contractor permit any such mechanisms to be shared or used by other than the individual Contractor personnel, subcontractor, or affiliate to whom issued. Contractor shall provide each Contractor personnel, subcontractors, or affiliates with only such level of access as is required for such individual to perform his or her assigned tasks and functions.

B. Throughout the Contract term, upon request from County but at least once each calendar year, Contractor shall provide County with an accurate, up-to-date list of those Contractor personnel and/or subcontractor personnel having access to County systems and/or County data, and the respective security level or clearance assigned to each such Contractor personnel and/or subcontractor personnel. County reserves the right to require the removal and replacement of Contractor personnel and/or subcontractor personnel at the County's sole discretion. Removal and replacement shall be performed within 14 calendar days of notification by the County.

C. All County resources (including County systems), County data, County hardware, and County software used or accessed by Contractor: (a) shall be used and accessed by such Contractor and/or subcontractors personnel solely and exclusively in the performance of their assigned duties in connection with, and in furtherance of, the performance of Contractor's obligations hereunder; and (b) shall not be used or accessed except as expressly permitted hereunder, or commercially exploited in any manner whatsoever, by Contractor or Contractor's personnel and subcontractors, at any time.

D. Contractor acknowledges and agrees that any failure to comply with the provisions of this paragraph shall constitute a breach of this Contract and entitle County to deny or restrict the rights of such non-complying Contractor personnel and/or subcontractor personnel to access and use the County data and/or system(s), as County in its sole discretion shall deem appropriate.

5. **Data Security Requirements:**

A. Without limiting Contractor's obligation of confidentiality as further described in this Contract, Contractor must establish, maintain, and enforce a data privacy program and an information and cyber security program, including safety, physical, and technical security and resiliency policies and procedures, that comply with the requirements set forth in this Contract and, to the extent such programs are consistent with and not less protective than the requirements set forth in this Contract and are at least equal to applicable best industry practices and standards (NIST 800-53).

B. Contractor also shall provide technical and organizational safeguards against accidental, unlawful, or unauthorized access or use, destruction, loss, alteration, disclosure, transfer, commingling, or processing of such information that ensure a level of security appropriate to the risks presented by the processing of County Data, Contractor personnel and/or subcontractor personnel and affiliates approved by County to perform work under this Contract may use or disclose County personal and confidential information only as permitted in this Contract. Any other use or disclosure requires express approval in writing by the County of Orange. No Contractor personnel and/or subcontractor personnel or affiliate shall duplicate, disseminate, market, sell, or disclose County personal and confidential information except as allowed in this Contract. Contractor personnel and/or subcontractor personnel or affiliate who access, disclose, market, sell, or use County personal and confidential information in a manner or for a purpose not authorized by this Contract may be subject to civil and criminal sanctions contained in applicable federal and state statutes.

C. Contractor shall take all reasonable measures to secure and defend all locations, equipment, systems, and other materials and facilities employed in connection with the Services against hackers and others who may seek, without authorization, to disrupt, damage, modify, access, or otherwise use Contractor systems or the information found therein; and prevent County data from being commingled with or contaminated by the data of other customers or their users of the Services and unauthorized access to any of County data.

D. Contractor shall also continuously monitor its systems for potential areas where security could be breached. In no case shall the safeguards of Contractor's data privacy and information and cyber security program be less stringent than the safeguards used by County. Without limiting any other audit rights of County, County shall have the right to review Contractor's data privacy and information and cyber security program prior to commencement of Services and from time to time during the term of this Contract.

E. All data belongs to the County and shall be destroyed or returned at the end of the contract via digital wiping, degaussing, or physical shredding as directed by County.

6. **Enhanced Security Measures:**

County may, in its discretion, designate certain areas, facilities, or solution systems as ones that require a higher level of security and access control. County shall notify Contractor in writing reasonably in advance of any such designation becoming effective. Any such notice shall set forth, in reasonable detail, the enhanced security or access-control procedures, measures, or requirements

that Contractor shall be required to implement and enforce, as well as the date on which such procedures and measures shall take effect. Contractor shall and shall cause Contractor personnel and subcontractors to fully comply with and abide by all such enhanced security and access measures and procedures as of such date.

7. **General Security Standards:**

Contractor will be solely responsible for the information technology infrastructure, including all computers, software, databases, electronic systems (including database management systems, email systems, auditing, and monitoring systems) and networks used by or for Contractor ("Contractor Systems") to access County resources (including County systems), County data or otherwise in connection with the Services and shall prevent unauthorized access to County resources (including County systems) or County data through the Contractor Systems.

A. **Contractor System(s) and Security:** At all times during the contract term, Contractor shall maintain a level of security with regard to the Contractor Systems, that in all events is at least as secure as the levels of security that are common and prevalent in the industry and in accordance with industry best practices (NIST 800-53). Contractor shall maintain all appropriate administrative, physical, technical, and procedural safeguards to secure County data from data breach, protect County data and the Services from loss, corruption, unauthorized disclosure, and from hacks, and the introduction of viruses, disabling devices, malware, and other forms of malicious and inadvertent acts that can disrupt County's access and use of County data and the Services.

B. **Contractor and the use of Email:** Contractor, including Contractor's employees and subcontractors, that are provided a County email address must only use the County email system for correspondence of County business. Contractor, including Contractor's employees and subcontractors, must not access or use personal, non-County Internet (external) email systems from County networks and/or County computing devices. If at any time Contractor's performance under this Contract requires such access or use, Contractor must submit a written request to County with justification for access or use of personal, non-County Internet (external) email systems from County networks and/or computing devices and obtain County's express prior written approval.

Contractors who are not provided with a County email address, but need to transmit County data will be required to maintain and transmit County data in accordance with this Agreement.

8. **Security Failures:**

Any failure by the Contractor to meet the requirements of this Contract with respect to the security of County data, including any related backup, disaster recovery, or other policies, practices or procedures, and any breach or violation by Contractor or its subcontractors or affiliates, or their employees or agents, of any of the foregoing, shall be deemed a material breach of this Contract and may result in termination and reimbursement to County of any fees prepaid by County prorated

to the date of such termination. The remedy provided in this paragraph shall not be exclusive and is in addition to any other rights and remedies provided by law or under the Contract.

9. **Security Breach Notification:**

A. In the event Contractor becomes aware of any act, error or omission, negligence, misconduct, or security incident including unsecure or improper data disposal, theft, loss, unauthorized use and disclosure or access, that compromises or is suspected to compromise the security, availability, confidentiality, and/or integrity of County data or the physical, technical, administrative, or organizational safeguards required under this Contract that relate to the security, availability, confidentiality, and/or integrity of County data, Contractor shall, at its own expense,

1. Immediately (or within 24 hours of potential or suspected breach), notify the County's Chief Information Security Officer and County Privacy Officer of such occurrence;
2. Perform a root cause analysis of the actual, potential, or suspected breach;
3. Provide a remediation plan that is acceptable to County within 30 days of verified breach, to address the occurrence of the breach and prevent any further incidents;
4. Conduct a forensic investigation to determine what systems, data, and information have been affected by such event; and
5. Cooperate with County and any law enforcement or regulatory officials investigating such occurrence, including but not limited to making available all relevant records, forensics, investigative evidence, logs, files, data reporting, and other materials required to comply with applicable law or as otherwise required by County and/or any law enforcement or regulatory officials, and
6. Perform or take any other actions required to comply with applicable law as a result of the occurrence (at the direction of County).

B. County shall make the final decision on notifying County officials, entities, employees, service providers, and/or the general public of such occurrence, and the implementation of the remediation plan. If notification to particular persons is required under any law or pursuant to any of County's privacy or security policies, then notifications to all persons and entities who are affected by the same event shall be considered legally required. Contractor shall reimburse County for all notification and related costs incurred by County arising out of or in connection with any such occurrence due to Contractor's acts, errors or omissions, negligence, and/or misconduct resulting in a requirement for legally required notifications.

C. In the case of a breach, Contractor shall provide third-party credit and identity monitoring services to each of the affected individuals for the period required to comply with applicable law, or, in the absence of any legally required monitoring services, for no less than 12 months following the date of notification to such individuals.

D. Contractor shall indemnify, defend with counsel approved in writing by County, and hold County and County Indemnitees harmless from and against any and all claims, including reasonable attorney's fees, costs, and expenses incidental thereto, which may be suffered

by, accrued against, charged to, or recoverable from County in connection with the occurrence.

Notification shall be sent to:

Andrew Alipanah, MBA, CISSP
Chief Information Security Officer
721 S. Parker St.
Suite 200
Orange, CA 92868
Phone: (714) 567-7611
Andrew.Alipanah@ocit.oc.gov

Linda Le, CHPC, CHC, CHP
County Privacy Officer
721 S. Parker St.
Suite 200
Orange, CA 92868
Phone: (714) 834-4082
Linda.Le@ocit.oc.gov

10. Security Audits:

A. Contractor shall maintain complete and accurate records relating to its system and Organization Controls (SOC) Type II audits or equivalent's data protection practices, internal and external audits, and the security of any of County-hosted content, including any confidentiality, integrity, and availability operations (data hosting, backup, disaster recovery, external dependencies management, vulnerability testing, penetration testing, patching, or other related policies, practices, standards, or procedures).

B. Contractor shall inform County of any internal/external security audit or assessment performed on Contractor's operations, information and cyber security program, disaster recovery plan, and prevention, detection, or response protocols that are related to hosted County content, within 60 calendar days of such audit or assessment. Contractor will provide a copy of the audit report to County within 30 days after Contractor's receipt of request for such report(s).

C. Contractor shall reasonably cooperate with all County security reviews and testing, including but not limited to penetration testing of any cloud-based solution provided by Contractor to County under this Contract. Contractor shall implement any required safeguards as identified by County or by any audit of Contractor's data privacy and information/cyber security program.

D. In addition, County has the right to review Plans of Actions and Milestones (POA&M) for any outstanding items identified by the SOC 2 Type II report requiring remediation as it pertains to the confidentiality, integrity, and availability of County data. County reserves the right, at its sole discretion, to immediately terminate this Contract or a part thereof

without limitation and without liability to County if County reasonably determines Contractor fails or has failed to meet its obligations under this section

11. Business Continuity and Disaster Recovery (BCDR):

A. For the purposes of this section, "Recovery Point Objectives" means the maximum age of files (data and system configurations) that must be recovered from backup storage for normal operations to resume if a computer, system, or network goes down as a result of a hardware, program, or communications failure (establishing the data backup schedule and strategy). "Recovery Time Objectives" means the maximum duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a loss of functionality.

B. The Contractor shall maintain a comprehensive risk management program focused on managing risks to County operations and data, including mitigation of the likelihood and impact of an adverse event occurring that would negatively affect contracted services and operations of the County. Business continuity management will enable the Contractor to identify and minimize disruptive risks and restore and recover hosted County business-critical services and/or data within the agreed terms following an adverse event or other major business disruptions. Recovery and timeframes may be impacted when events or disruptions are related to dependencies on third parties. The County and Contractor will agree on Recovery Point Objectives and Recovery Time Objectives (as needed) and will periodically review these objectives. Any disruption to services of system will be communicated to the County within 4 hours, and every effort shall be undertaken to restore contracted services, data, operations, security, and functionality.

C. All data and/or systems and technology provided by the Contractor internally and through third-party vendors shall have resiliency and redundancy capabilities to achieve high availability and data recoverability. Contractor Systems shall be designed, where practical and possible, to ensure continuity of service(s) in the event of a disruption or outage.

ATTACHMENT B

OCSSA STATE PRIVACY AND SECURITY PROVISIONS

DEFINITIONS

For the purpose of this Agreement, the following terms mean:

1. "**Assist in the administration of the Medi-Cal program**" means performing administrative functions on behalf of Medi-Cal programs, such as establishing eligibility, determining the amount of medical assistance, and collecting PII for such purposes, to the extent such activities are authorized by law.

2. "**Breach**" refers to actual loss, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for other than authorized purposes have access or potential access to PII, whether electronic, paper, verbal, or recorded.

3. "**Contractor Worker**" means those Contractor employees, contractors, subcontractors, vendors and agents performing any functions for the Contractor that require access to and/or use of PII and that are authorized by the Contractor to access and use PII. An agent is a person or organization authorized to act on behalf of the Contractor.

4. "**PII**" includes "**Medi-Cal PII**" and is defined as personally identifiable information directly obtained in the course of performing an administrative function through the MEDS or IEVS systems on behalf of Medi-Cal programs that can be used alone, or in conjunction with any other information, to identify a specific individual. PII includes any information that can be used to search for or identify individuals, or can be used to access their files, including but not limited to name, social security number (SSN), date and place of birth (DOB), mother's maiden name, driver's license number, or identification number. PII may also include any information that is linkable to an individual, such as medical, educational, financial, and employment information. PII may be electronic, paper, verbal, or recorded and includes statements made by, or attributed to, the individual.

5. "**Security Incident**" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of PII, or interference with system operations in an information system which processes PII that is under the control of the County or California Statewide Automated Welfare System (CalSAWS) Consortium, or a contractor, subcontractor or vendor of the County.

6. "**Secure Areas**" means any area where:
   A. Contractor Workers assist in the administration of Medi-Cal programs;
   B. Contractor Workers use or disclose PII; or
   C. PII is stored in paper or electronic format.

7. "**SSA-provided or verified data (SSA data)**" means:

   A. Any information under the control of the Social Security Administration (SSA) provided to Department of Health Care Services (DHCS) and California Department of Social Services (CDSS)

under the terms of an information exchange agreement with SSA (e.g., SSA provided date of death, SSA Title II or Title XVI benefit and eligibility data, or SSA citizenship verification); or

B. Any information provided to the County of Orange by DHCS and CDSS, including a source other than SSA, but in which DHCS and CDSS attests that SSA verified it, or couples the information with data from SSA to certify the accuracy of it (e.g., SSN and associated SSA verification indicator displayed together on a screen, file, or report, or DOB and associated SSA verification indicator displayed together on a screen, file, or report).

AGREEMENTS

County of Orange and Contractor mutually agree as follows:

I. PRIVACY AND CONFIDENTIALITY

A. Contractor Workers may use or disclose PII only as permitted in this Agreement and only to assist in the administration of Medi-Cal programs in accordance with Section 14100.2 of the Welfare and Institutions Code, Section 431.302 of Title 42 Code of Federal Regulations, as limited by this Agreement, and as otherwise required by law. Disclosures required by law or that are made with the explicit written authorization of the client, such as through an authorized release of information form, are allowable. Any other use or disclosure of PII requires the express approval in writing of County of Orange. No Contractor Worker shall duplicate, disseminate or disclose PII except as allowed in this Agreement.

B. While County of Orange is a hybrid covered entity under the federal Health Insurance Portability and Accountability Act, as amended from time to time (HIPAA), the Contractor is not required to be the business associate of the County of Orange, if the activities of the Contractor are limited to determining eligibility for, or enrollment in, Medi-Cal programs (45 CFR 160.103). Nevertheless, it is the intention of the parties to protect the privacy and security of PII and the rights of Medi-Cal applicants and beneficiaries in a manner that is consistent with HIPAA and other laws that are applicable. It is not the intention of the parties to voluntarily subject the Contractor to federal HIPAA jurisdiction where it would not otherwise apply.
   1. To the extent that other state and/or federal laws provide additional, stricter, and/or more protective (collectively, more protective) privacy and/or security protections to the PII covered under this Agreement beyond those provided through HIPAA, as applicable, Contractor shall:

      a. Comply with the more protective of the privacy and security standards set forth in applicable state or federal laws to the extent such standards provide a greater degree of protection and security than HIPAA or are otherwise more favorable to the individuals whose information is concerned; and
      b. Treat any violation of such additional and/or more protective standards as a breach or security incident, as appropriate, pursuant to Section VIII. of this Agreement. It is not the intention of the parties that this subsection I.B.(1)(b) expands the definitions of breach nor security incident set forth this Agreement unless the additional and/or more protective standard has a different definition for these terms, as applicable.

Examples of laws that provide additional and/or stricter privacy protections to certain types of PII include but are not limited to the Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR Part 2, Welfare and Institutions Code section 5328, and California Health and Safety Code section 11845.5.

C. Access to PII shall be restricted to Contractor Workers who need to perform their official duties to assist in the administration of Medi-Cal programs.

D. Contractor Workers who access, disclose or use PII in a manner or for a purpose not authorized by this Agreement may be subject to civil and criminal sanctions contained in applicable federal and state statutes.

II. PERSONNEL CONTROLS

The Contractor agrees to advise Contractor Workers who have access to PII of the confidentiality of the information, the safeguards required to protect the information, and the civil and criminal sanctions for non-compliance contained in applicable federal and state laws. For that purpose, the Contractor shall implement the following personnel controls:

A. ***Employee Training.*** Train and use reasonable measures to ensure compliance with the requirements of this Agreement by Contractor Workers, including, but not limited to:

1. Provide initial privacy and security awareness training to each new Contractor Worker within 30 days of employment;

2. Thereafter, provide annual refresher training or reminders of the privacy and security safeguards in this Agreement to all Contractor Workers. Three or more security reminders per year are recommended;

3. Maintain records indicating each Contractor Worker's name and the date on which the privacy and security awareness training was completed and;

4. Retain training records for a period of five years after completion of the training.

B. ***Employee Discipline.***

1. Provide documented sanction policies and procedures for Contractor Workers who fail to comply with privacy policies and procedures or any provisions of these requirements.

2. Sanction policies and procedures shall include termination of employment when appropriate.

C. ***Confidentiality Statement.*** Ensure that all Contractor Workers sign a confidentiality statement. The statement shall be signed by Contractor Workers prior to accessing PII and annually thereafter. Signatures may be physical or electronic. The signed statement shall be retained for a period of five years.

The statement shall include, at a minimum, a description of the following:

1. General Use of PII;
2. Security and Privacy Safeguards for PII;
3. Unacceptable Use of PII; and
4. Enforcement Policies.

D. ***Background Screening.***

1. Conduct a background screening of a Contractor Worker before they may access PII.

2. The background screening should be commensurate with the risk and magnitude of harm the employee could cause. More thorough screening shall be done for those employees who are authorized to bypass significant technical and operational security controls.

3. The Contractor shall retain each Contractor Worker's background screening documentation for a period of three years following conclusion of employment relationship.

III. MANAGEMENT OVERSIGHT AND MONITORING

To ensure compliance with the privacy and security safeguards in this Agreement the Contractor shall perform the following:

A. Conduct periodic privacy and security review of work activity by Contractor Workers, including random sampling of work product. Examples include, but are not limited to, access to case files or other activities related to the handling of PII.

The periodic privacy and security reviews shall be performed or overseen by management level personnel who are knowledgeable and experienced in the areas of privacy and information security in the administration of the Medi-Cal program and the use or disclosure of PII.

B. Utilize Medi-Cal Eligibility Data System (MEDS) audit reports provided by the County of Orange and other system auditing tools available to Contractor to perform quality assurance and management oversight reviews of their Contractor Workers' access to Medi-Cal and SSA PII within data systems utilized, including MEDS. For additional information see Medi-Cal Eligibility Division Information Letter | 21-34. Any instances of suspected security incidents or breaches are to be reported to the County of Orange immediately following the instructions within Section X of this Agreement.

To ensure a separation of duties, these system audit reviews shall be performed by privacy and security staff who do not have access to PII within the systems. DHCS requires the County of Orange to enforce a separation of duties, excluding any individual who uses MEDS to make benefit or entitlement determinations from participating in oversight, monitoring, or quality assurance functions. The County of Orange acknowledges that with smaller contractors the separation of duties requirement might create a hardship based on there being a small number of people available to perform various tasks. Requests for hardship exemptions will be approved on a case-by-case basis.

IV. INFORMATION SECURITY AND PRIVACY STAFFING

The Contractor agrees to:

A. Designate information security and privacy officials who are accountable for compliance with these and all other applicable requirements stated in this Agreement.

B. Provide the County of Orange with applicable contact information for these designated individuals using the County inbox listed in Section IX of this Agreement. Any changes to this information should be reported to the County of Orange within 10 days.

C. Assign Contractor Workers to be responsible for administration and monitoring of all security-related controls stated in this Agreement.

V. TECHNICAL SECURITY CONTROLS

The State of California Office of Information Security (OIS) and SSA have adopted the National Institute of Standards and Technology (NIST) Special Publication (SP) 800- 53, Security and Privacy controls for Information Systems and Organizations, and NIST SP 800-37, Risk Management Framework for Information Systems and Organizations.

OIS and SSA require organizations to comply and maintain the minimum standards outlined in NIST SP 800-53 when working with PII and SSA data. Contractor shall, at a minimum, implement an information security program that effectively manages risk in accordance with the Systems Security Standards and Requirements outlined in this Section of this Agreement.

Guidance regarding implementation of NIST SP 800-53 is available in the Statewide Information Management Manual (SIMM), SIMM-5300-A, which is hereby incorporated into this Agreement (Exhibit C) and available upon request.

The County of Orange will enter into a separate PSA with California Statewide Automated Welfare System (CalSAWS) Joint Powers Authority specific to the CalSAWS. Any requirements for data systems in this PSA would only apply to Contractor's locally operated/administered systems that access, store, or process PII.

[Remainder of page intentionally left blank]

A. Systems Security Standards and Requirements

1. **Access Control (AC)**

Control Number	AC-1
Title	Access Control Policy and Procedures
DHCS & CDSS Requirement	The organization must: a. Develop, document, and disseminate to designated organization officials: 1. An access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; 2. Procedures to facilitate the implementation of the access control policy and associated access control controls; b. Review and update the current access control procedures with the organization-defined frequency.
Supplemental Guidance (from NIST 800-53)	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AC family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.
Control Number	AC-2
Title	Account Management
DHCS & CDSS Requirement	The organization must: a. Identify and select the accounts with access to PII to support organizational missions/business functions. b. Assign account managers for information system accounts; c. Establish conditions for group and role membership; d. 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; e. Require approvals by designated access authority for requests to create information system accounts; f. Create, enable, modify, disable, and remove information system accounts in accordance with organization account management procedures; g. Monitors the use of information system accounts; h. Notifies account managers when accounts are no longer required, when users are terminated or transferred; and when individual information system usage or need-to-know changes.

	i. Authorizes access to the information systems that receive, process, store or transmit PII based on valid access authorization, need-to-know permission or under the authority to re- disclose PII. j. Review accounts for compliance with account management requirements according to organization-based frequency; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.
Supplemental Guidance (from NIST 800-53)	Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local logon accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when individuals are transferred or terminated. Some types of information system accounts may require specialized training. Related controls: AC- 3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PL-4, SC-13.
Control Number	AC-3
Title	Account Management
DHCS & CDSS Requirement	The organization must: a. Identify and select the accounts with access to PII to support organizational missions/business functions. b. Assign account managers for information system accounts; c. Establish conditions for group and role membership; d. 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;

	e. Require approvals by designated access authority for requests to create information system accounts; f. Create, enable, modify, disable, and remove information system accounts in accordance with organization account management procedures; g. Monitors the use of information system accounts; h. Notifies account managers when accounts are no longer required, when users are terminated or transferred; and when individual information system usage or need-to-know changes. i. Authorizes access to the information systems that receive, process, store or transmit PII based on valid access authorization, need-to-know permission or under the authority to re- disclose PII. j. Review accounts for compliance with account management requirements according to organization-based frequency; and k. Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group.
Supplemental Guidance (from NIST 800-53)	Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service. Some of the account management requirements listed above can be implemented by organizational information systems. The identification of authorized users of the information system and the specification of access privileges reflects the requirements in other security controls in the security plan. Users requiring administrative privileges on information system accounts receive additional scrutiny by appropriate organizational personnel (e.g., system owner, mission/business owner, or chief information security officer) responsible for approving such accounts and privileged access. Organizations may choose to define access privileges or other attributes by account, by type of account, or a combination of both. Other attributes required for authorizing access include, for example, restrictions on time-of-day, day-of-week, and point-of-origin. In defining other account attributes, organizations consider system-related requirements (e.g., scheduled maintenance, system upgrades) and mission/business requirements, (e.g., time zone differences, customer requirements, remote access to support travel requirements). Failure to consider these factors could affect information system availability. Temporary and emergency accounts are accounts intended for short-term use. Organizations establish temporary accounts as a part of normal account activation procedures when there is a need for short-term accounts without the demand for immediacy in account activation. Organizations establish emergency accounts in response to crisis situations and with the need for rapid account activation. Therefore, emergency account activation may bypass normal account authorization processes. Emergency and temporary accounts are not to be confused with infrequently used accounts (e.g., local logon accounts used for special tasks defined by organizations or when network resources are unavailable). Such accounts remain available and are not subject to automatic disabling or removal dates. Conditions for disabling or deactivating accounts include, for example: (i) when shared/group, emergency, or temporary accounts are no longer required; or (ii) when individuals are transferred or terminated. Some types of information system accounts may require specialized training. Related controls: AC- 3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-2, IA-4, IA-5, IA-8, CM-5, CM-6, CM-11, MA-3, MA-4, MA-5, PL-4, SC-13.
Control Number	AC-3(7)
Title	Access Enforcement | Role-Based Access Control

DHCS & CDSS Requirement	The organization information system must: enforce a role-based access control policy over defined subjects and objects and controls access based upon the need to utilize PII.
Supplemental Guidance (from NIST 800-53)	Role-based access control (RBAC) is an access control policy that restricts information system access to authorized users. Organizations can create specific roles based on job functions and the authorizations (i.e., privileges) to perform needed operations on organizational information systems associated with the organization-defined roles. When users are assigned to the organizational roles, they inherit the authorizations or privileges defined for those roles. RBAC simplifies privilege administration for organizations because privileges are not assigned directly to every user (which can be a significant number of individuals for mid- to large-size organizations) but are instead acquired through role assignments. RBAC can be implemented either as a mandatory or discretionary form of access control. For organizations implementing RBAC with mandatory access controls, the requirements in AC-3 (3) define the scope of the subjects and objects covered by the policy.
Control Number	AC-3(8)
Title	Access Enforcement | Revocation of Access Authorization
DHCS & CDSS Requirement	The organization must: Enforce a role-based access control over users and information resources that have access to PII, and control access based upon organization defined roles and users authorized to assume such roles.
Supplemental Guidance (from NIST 800-53)	Revocation of access rules may differ based on the types of access revoked. For example, if a subject (i.e., user or process) is removed from a group, access may not be revoked until the next time the object (e.g., file) is opened or until the next time the subject attempts a new access to the object. Revocation based on changes to security labels may take effect immediately. Organizations can provide alternative approaches on how to make revocations immediate if information systems cannot provide such capability and immediate revocation is necessary.
Control Number	AC-4
Title	Information Flow Enforcement
DHCS & CDSS Requirement	The organization information system must: enforce approved authorizations for controlling the flow of information within the system and between interconnected systems based on the need for interconnected systems to share PII to conduct business.
Supplemental Guidance (from NIST 800-53)	Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. Flow control restrictions include, for example, keeping export-controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, restricting web requests to the Internet that are not from the internal web proxy server, and limiting information transfers between organizations based on data structures and content. Transferring information between information systems representing different security domains with different security policies introduces risk that such transfers violate one or more domain security policies. In such situations, information owners/stewards provide guidance at designated policy enforcement points between interconnected systems. Organizations consider mandating specific architectural solutions when required to enforce specific security policies.

	Enforcement includes, for example: (i) prohibiting information transfers between interconnected systems (i.e., allowing access only); (ii) employing hardware mechanisms to enforce one-way information flows; and (iii) implementing trustworthy regrading mechanisms to reassign security attributes and security labels. Organizations commonly employ information flow control policies and enforcement mechanisms to control the flow of information between designated sources and destinations (e.g., networks, individuals, and devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Enforcement occurs, for example, in boundary protection devices (e.g., gateways, routers, guards, encrypted tunnels, firewalls) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message- filtering capability based on message content (e.g., implementing key word searches or using document characteristics). Organizations also consider the trustworthiness of filtering/inspection mechanisms (i.e., hardware, firmware, and software components) that are critical to information flow enforcement. Control enhancements 3 through 22 primarily address cross-domain solution needs which focus on more advanced filtering techniques, in-depth analysis, and stronger flow enforcement mechanisms implemented in cross-domain products, for example, high-assurance guards. Such capabilities are generally not available in commercial off-the-shelf information technology products. Related controls: AC-3, AC-17, AC-19, AC-21, CM-6, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18
Control Number	AC-5
Title	Separation of Duties
DHCS & CDSS Requirement	The organization must: a. Separate organization-defined duties of individuals; b. Document separation of duties of individuals; and c. Defines information system access authorizations to support separation of duties. *DHCS and CDSS also require that the state organization prohibit any functional component(s) or official(s) from issuing credentials or access authority to themselves or other individuals within their job- function or category of access.* *Federal requirements and DHCS and CDSS policy exclude any employee who uses PII to process programmatic workloads to make benefit or entitlement determinations from participation in management or quality assurance functions.*
Supplemental Guidance (from NIST 800-53)	Separation of duties addresses the potential for abuse of authorized privileges and helps to reduce the risk of malevolent activity without collusion. Separation of duties includes, for example: (i) dividing mission functions and information system support functions among different individuals and/or roles; (ii) conducting information system support functions with different individuals (e.g., system management, programming, configuration management, quality assurance and testing, and network security); and (iii) ensuring security personnel administering access control functions do not also administer audit functions. Related controls: AC-3, AC-6, PE-3, PE-4, PS-2.
Control Number	AC-6
Title	Least Privilege
DHCS & CDSS	The organization must:

Requirement	Employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.
Supplemental Guidance (from NIST 800-53)	Organizations employ least privilege for specific duties and information systems. The principle of least privilege is also applied to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions/business functions. Organizations consider the creation of additional processes, roles, and information system accounts as necessary, to achieve least privilege. Organizations also apply least privilege to the development, implementation, and operation of organizational information systems. Related controls: AC-2, AC-3, AC-5, CM-6, CM-7, PL-2.
Control Number	AC-6(1)
Title	Least Privilege | Authorize Access to Security Functions
DHCS & CDSS Requirement	The organization must explicitly authorize access to organization-defined security functions (deployed in hardware, software, and firmware) and security-relevant information.
Supplemental Guidance (from NIST 800-53)	Security functions include, for example, establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters. Security-relevant information includes, for example, filtering rules for routers/firewalls, cryptographic key management information, configuration parameters for security services, and access control lists. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users.
Control Number	AC-6(7)
Title	Least Privilege | Review Of User Privileges
DHCS & CDSS Requirement	The organization must: a. Review the privileges assigned to organization-defined roles or classes of users to validate the need for such privileges; and b. Reassign or removes privileges, if necessary, to correctly reflect organizational mission/business needs.
Supplemental Guidance (from NIST 800-53)	The need for certain assigned user privileges may change over time reflecting changes in organizational missions/business function, environments of operation, technologies, or threat. Periodic review of assigned user privileges is necessary to determine if the rationale for assigning such privileges remains valid. If the need cannot be revalidated, organizations take appropriate corrective actions. Related control: CA-7.
Control Number	AC-7
Title	Unsuccessful Logon Attempts
DHCS & CDSS Requirement	The organization must: a. Enforce a limit of no fewer than three (3) and no greater than five (5) consecutive invalid logon attempts by a user during an organization-defined time period; and b. Automatically lock the account/node for: an organization-defined time period; or locks the account/node until released by an administrator; or delays next logon prompt according to organization-defined delay algorithm when the maximum number of unsuccessful attempts is exceeded.

Supplemental Guidance (from NIST 800-53)	This control applies regardless of whether the logon occurs via a local or network connection. Due to the potential for denial of service, automatic lockouts initiated by information systems are usually temporary and automatically release after a predetermined time period established by organizations. If a delay algorithm is selected, organizations may choose to employ different algorithms for different information system components based on the capabilities of those components. Responses to unsuccessful logon attempts may be implemented at both the operating system and the application levels. Related controls: AC-2, AC-9, AC-14, IA-5.
Control Number	AC-8
Title	System Use Notification
DHCS & CDSS Requirement	The organization must: a. Displays to users system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance and states that: 1. Users are accessing a U.S. Government information system; 2. Information system usage may be monitored, recorded, and subject to audit; 3. Unauthorized use of the information system is prohibited and subject to criminal and civil penalties; and 4. Use of the information system indicates consent to monitoring and recording; b. Retains the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the information system; and c. For publicly accessible systems: 1. Displays system use information organization-defined conditions, before granting further access; 2. Displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. Includes a description of the authorized uses of the system. At a minimum, this can be done at initial logon and is not required for every logon.
Supplemental Guidance (from NIST 800-53)	System use notifications can be implemented using messages or warning banners displayed before individuals log in to information systems. System use notifications are used only for access via logon interfaces with human users and are not required when such human interfaces do not exist. Organizations consider system use notification messages/banners displayed in multiple languages based on specific organizational needs and the demographics of information system users. Organizations also consult with the Office of the General Counsel for legal review and approval of warning banner content.
Control Number	AC-11
Title	Session Lock
DHCS & CDSS Requirement	The organization's information system: a. Prevents further access to the system by initiating a session lock after 15 minutes or upon receiving a request from a user; and b. Retains the session lock until the user reestablishes access using established identification

	and authentication procedures.
Supplemental Guidance (from NIST 800-53)	Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. Session locks are not an acceptable substitute for logging out of information systems, for example, if organizations require users to log out at the end of workdays. Related control: AC-7.
Control Number	AC-17
Title	Remote Access
DHCS & CDSS Requirement	The organization must: a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and b. Authorize remote access to the information system prior to allowing such connections.
Supplemental Guidance (from NIST 800-53)	Remote access is access to organizational information systems by users (or processes acting on behalf of users) communicating through external networks (e.g., the Internet). Remote access methods include, for example, dial-up, broadband, and wireless. Organizations often employ encrypted virtual private networks (VPNs) to enhance confidentiality and integrity over remote connections. The use of encrypted VPNs does not make the access non-remote; however, the use of VPNs, when adequately provisioned with appropriate security controls (e.g., employing appropriate encryption techniques for confidentiality and integrity protection) may provide sufficient assurance to the organization that it can effectively treat such connections as internal networks. Still, VPN connections traverse external networks, and the encrypted VPN does not enhance the availability of remote connections. Also, VPNs with encrypted tunnels can affect the organizational capability to adequately monitor network communications traffic for malicious code. Remote access controls apply to information systems other than public web servers or systems designed for public access. This control addresses authorization prior to allowing remote access without specifying the formats for such authorization. While organizations may use interconnection security agreements to authorize remote access connections, such agreements are not required by this control. Enforcing access restrictions for remote connections is addressed in AC-3. Related controls: AC-2, AC-3, AC-18, AC-19, AC-20, CA-3, CA-7, CM-8, IA-2, IA-3, IA-8, MA-4, PE-17, PL-4, SC-10, SI-4.

2. **Accountability, Audit, and Risk Management (AR)**

Control Number	AR-3
Title	Privacy Requirements for Contractors and Service Providers
DHCS & CDSS Requirement	The organization must: a. Establish privacy roles, responsibilities, and access requirements for contractors and service providers; and b. Includes privacy requirements in contracts and other acquisition-related documents.
Supplemental Guidance (from NIST 800-53)	Contractors and service providers include, but are not limited to, information providers, information processors, and other organizations providing information system development, information technology services, and other outsourced applications. Organizations consult with legal counsel, the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO), and

	contracting officers about applicable laws, directives, policies, or regulations that may impact implementation of this control. Related control: AR-1, AR-5, SA-4.

3. Audit and Accountability (AU)

Control Number	AU-1
Title	Audit and Accountability Policy and Procedures
DHCS & CDSS Requirement	The organization must: a. Develop, document, and disseminate to individuals and organizations that store, process, or transmit PII: 1. An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and b. Review and update the current: 1. Audit and accountability policy at least triennially; and 2. Audit and accountability procedures at least triennially.
Supplemental Guidance (from NIST 800-53)	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AU family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.
Control Number	AU-2
Title	Audit Events
DHCS & CDSS Requirement	The organization must: a. Audit the following events: 1. Viewing PII stored within the organization's system; 2. Viewing of screens that contain PII; 3. All system and data interactions concerning PII. b. Coordinate the security audit function with other organizational entities requiring audit-related information to enhance mutual support and to help guide the selection of auditable events; c. Determines that the following events are to be audited within the information system: 1. Viewing PII stored within the organization's system; 2. Viewing of screens that contain PII; 3. All system and data interactions concerning PII.

Supplemental Guidance (from NIST 800-53)	An event is any observable occurrence in an organizational information system. Organizations identify audit events as those events which are significant and relevant to the security of information systems and the environments in which those systems operate in order to meet specific and ongoing audit needs. Audit events can include, for example, password changes, failed logons, or failed accesses related to information systems, administrative privilege usage, PIV credential usage, or third-party credential usage. In determining the set of auditable events, organizations consider the auditing appropriate for each of the security controls to be implemented. To balance auditing requirements with other information system needs, this control also requires identifying that subset of auditable events that are audited at a given point in time. For example, organizations may determine that information systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance. Auditing requirements, including the need for auditable events, may be referenced in other security controls and control enhancements. Organizations also include auditable events that are required by applicable federal laws, Executive Orders, directives, policies, regulations, and standards. Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of auditable events, the auditing necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented architectures. Related controls: AC-6, AC-17, AU-3, AU-12, MA-4, MP-2, MP-4, SI-4
Control Number	AU-11
Title	Audit Record Retention
DHCS & CDSS Requirement	The organization must retain audit records for six (6) years to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.
Supplemental Guidance (from NIST 800-53)	Organizations retain audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoenas, and law enforcement actions. Organizations develop standard categories of audit records relative to such types of actions and standard response processes for each type of action. The National Archives and Records Administration (NARA) General Records Schedules provide federal policy on record retention. Related controls: AU-4, AU-5, AU-9, MP-6.
Control Number	AU-12
Title	Audit Generation
DHCS & CDSS Requirement	The organization information system must: a. Provide audit record generation capability for the auditable events defined in AU-2 a. at the audit reporting mechanism; b. Allow security personnel to select which auditable events are to be audited by specific components of the information system; and c. Generates audit records for the events defined in AU-2 d. with the content defined in AU-3
Supplemental Guidance (from	Audit records can be generated from many different information system components. The list of audited events is the set of events for which audits are to be generated. These events are typically

NIST 800-53)	a subset of all events for which the information system is capable of generating audit records. Related controls: AC-3, AU-2, AU-3, AU-6, AU-7.

4. **Awareness and Training (AT)**

Control Number	AT-1
Title	Security Awareness and Training Policy and Procedures
DHCS & CDSS Requirement	The organization must: a. Develop, document, and disseminate to personnel and organizations with access to PII: 1. A security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls; and b. Reviews and updates the current: 1. Security awareness and training policy and; 2. Security awareness and training procedures. The training and awareness programs must include: The sensitivity of PII, The rules of behavior concerning use and security in systems and/or applications processing PII, The Privacy Act and other Federal and state laws, including but not limited to Section 14100.2 of the Welfare and Institutions Code and Section 431.302 et. Seq. of Title 42 Code of Federal Regulations, governing collection, maintenance, use, and dissemination of information about individuals, The possible criminal and civil sanctions and penalties for misuse of PII, The responsibilities of employees, contractors, and agent's pertaining to the proper use and protection of PII, The restrictions on viewing and/or copying PII, The proper disposal of PII, The security breach and data loss incident reporting procedures, The basic understanding of procedures to protect the network from viruses, worms, Trojan horses, and other malicious code, Social engineering (phishing, vishing and pharming) and network fraud prevention.
Supplemental Guidance (from NIST 800-53)	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the AT family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The

	organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.
Control Number	AT-2
Title	Security Awareness Training
DHCS & CDSS Requirement	The organization must provide basic security awareness training to information system users (including managers, senior executives, and contractors): a. As part of initial training for new users; b. When required by information system changes; and c. Annually thereafter.
Supplemental Guidance (from NIST 800-53)	Organizations 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 includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses 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. Related controls: AT-3, AT-4, PL-4.
Control Number	AT-3
Title	Role-Based Security Training
DHCS & CDSS Requirement	The organization must provide role-based security training to personnel with assigned security roles and responsibilities: a. Before authorizing access to the information system or performing assigned duties; b. When required by information system changes; and c. With organization-defined frequency thereafter.
Supplemental Guidance (from NIST 800-53)	Organizations determine the appropriate content of security training based on the assigned roles and responsibilities of individuals and the specific security requirements of organizations and the information systems to which personnel have authorized access. In addition, organizations provide enterprise architects, information system developers, software developers, acquisition/procurement officials, information system managers, system/network administrators, personnel conducting configuration management and auditing activities, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training specifically tailored for their assigned duties. Comprehensive role-based training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. Such training can include for example, policies, procedures, tools, and artifacts for the organizational security roles defined. Organizations also provide the training necessary for individuals to carry out their responsibilities related to operations and supply chain security within the context of organizational information security programs. Role- based security training also applies to contractors providing services to federal agencies. Related controls: AT-2, AT-4, PL-4, PS-7, SA-3, SA-12, SA-16.
Control Number	AT-4
Title	Security Training Records

DHCS & CDSS Requirement	The organization must: a. Document and monitor individual information system security training activities including basic security awareness training and specific information system security training; and b. Retain individual training records for 5 years. SSA also requires the organization to certify that each employee, contractor, and agent who views SSA data certify that they understand the potential criminal, civil, and administrative sanctions or penalties for unlawful assess and/or disclosure.
Supplemental Guidance (from NIST 800-53)	Documentation for specialized training may be maintained by individual supervisors at the option of the organization. Related controls: AT-2, AT-3, PM-14.

5. **Contingency Planning (CP)**

Control Number	CP-2
Title	Contingency Plan
DHCS & CDSS Requirement	The organization must: a. Develop a contingency plan for the information system that: 1. Identifies essential missions and business functions and associated contingency requirements; 2. Provides recovery objectives, restoration priorities, and metrics; 3. Addresses contingency roles, responsibilities, assigned individuals with contact information; 4. Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure; 5. Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and 6. Is reviewed and approved by a senior manager; b. Distribute copies of the contingency plan to personnel and organizations supporting the contingency plan actions; c. Coordinate contingency planning activities with incident handling activities; d. Review the contingency plan for the information system at least annually; e. Update the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; f. Communicate contingency plan changes to personnel and organizations supporting the contingency plan actions; g. Incorporate lessons learned from contingency plan testing, training, or actual contingency activities into contingency testing and training; and h. Protect the contingency plan from unauthorized disclosure and modification.
Supplemental Guidance (from NIST 800-53)	Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. The effectiveness of contingency planning is maximized by

	considering such planning throughout the phases of the system development life cycle. Performing contingency planning on hardware, software, and firmware development can be an effective means of achieving information system resiliency. Contingency plans reflect the degree of restoration required for organizational information systems since not all systems may need to fully recover to achieve the level of continuity of operations desired. Information system recovery objectives reflect applicable laws, Executive Orders, directives, policies, standards, regulations, and guidelines. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission and/or business effectiveness, such as malicious attacks compromising the confidentiality or integrity of information systems. Actions addressed in contingency plans include, for example, orderly/graceful degradation, information system shutdown, fallback to a manual mode, alternate information flows, and operating in modes reserved for when systems are under attack. By closely coordinating contingency planning with incident handling activities, organizations can ensure that the necessary contingency planning activities are in place and activated in the event of a security incident. Related controls: AC-14, CP-6, CP-7, CP-8, CP-9, CP-10, IR-4, IR-8, MP-2, MP-4, MP-5, PM-8, PM-11.

6. **Data Minimization and Retention (DM)**

Control Number	DM-2
Title	Data Retention and Disposal
DHCS & CDSS Requirement	The organization must: a. Retain each collection of PII no longer than required for the organization's business process or evidentiary purposes; b. Dispose of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and c. Use organization-defined techniques or methods to ensure secure deletion or destruction of PII (including originals, copies, and archived records).
Supplemental Guidance (from NIST 800-53)	NARA provides retention schedules that govern the disposition of federal records. Program officials coordinate with records officers and with NARA to identify appropriate retention periods and disposal methods. NARA may require organizations to retain PII longer than is operationally needed. In those situations, organizations describe such requirements in the notice. Methods of storage include, for example, electronic, optical media, or paper. Examples of ways organizations may reduce holdings include reducing the types of PII held (e.g., delete Social Security numbers if their use is no longer needed) or shortening the retention period for PII that is maintained if it is no longer necessary to keep PII for long periods of time (this effort is undertaken in consultation with an organization's records officer to receive NARA approval). In both examples, organizations provide notice (e.g., an updated System of Records Notice) to inform the public of any changes in holdings of PII. Certain read-only archiving techniques, such as DVDs, CDs, microfilm, or microfiche, may not permit the removal of individual records without the destruction of the entire database contained on such media. Related controls: AR-4, AU-11, DM-1, MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SI-12, TR-1.

7. Identification and Authentication (IA)

Control Number	IA-2
Title	Identification and Authentication (Organizational Users)
DHCS & CDSS Requirement	The organization's information system must uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).
Supplemental Guidance (from NIST 800-53)	Organizational users include employees or individuals that organizations deem to have equivalent status of employees (e.g., contractors, guest researchers). This control applies to all accesses other than: (i) accesses that are explicitly identified and documented in AC-14; and (ii) accesses that occur through authorized use of group authenticators without individual authentication. Organizations may require unique identification of individuals in group accounts (e.g., shared privilege accounts) or for detailed accountability of individual activity. Organizations employ passwords, tokens, or biometrics to authenticate user identities, or in the case multifactor authentication, or some combination thereof. Access to organizational information systems is defined as either local access or network access. Local access is any access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained by direct connections without the use of networks. Network access is access to organizational information systems by users (or processes acting on behalf of users) where such access is obtained through network connections (i.e., nonlocal accesses). Remote access is a type of network access that involves communication through external networks (e.g., the Internet). Internal networks include local area networks and wide area networks. In addition, the use of encrypted virtual private networks (VPNs) for network connections between organization-controlled endpoints and non-organization controlled endpoints may be treated as internal networks from the perspective of protecting the confidentiality and integrity of information traversing the network. Organizations can satisfy the identification and authentication requirements in this control by complying with the requirements in Homeland Security Presidential Directive 12 consistent with the specific organizational implementation plans. Multifactor authentication requires the use of two or more different factors to achieve authentication. The factors are defined as: (i) something you know (e.g., password, personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government Personal Identity Verification card and the DoD common access card. In addition to identifying and authenticating users at the information system level (i.e., at logon), organizations also employ identification and authentication mechanisms at the application level, when necessary, to provide increased information security. Identification and authentication requirements for other than organizational users are described in IA-8. Related controls: AC-2, AC-3, AC-14, AC-17, AC-18, IA-4, IA-5, IA-8.
Control Number	IA-5
Title	Authenticator Management
DHCS & CDSS Requirement	The organization must manage information system authenticators by: a. Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator;

	b. Establishing initial authenticator content for authenticators defined by the organization; c. Ensuring that authenticators have sufficient strength of mechanism for their intended use; d. Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; e. Changing default content of authenticators prior to information system installation; f. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g. Changing/refreshing authenticators within organization-defined time period; h. Protecting authenticator content from unauthorized disclosure and modification; i. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and j. Changing authenticators for group/role accounts when membership to those accounts changes.
Supplemental Guidance (from NIST 800-53)	Individual authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). In many cases, developers ship information system components with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, and present a significant security risk. The requirement to protect individual authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of individuals and by controls AC-3, AC-6, and SC-28 for authenticators stored within organizational information systems (e.g., passwords stored in hashed or encrypted formats, files containing encrypted or hashed passwords accessible with administrator privileges). Information systems support individual authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one-time tokens, and number of allowed rejections during the verification stage of biometric authentication. Specific actions that can be taken to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords. Related controls: AC-2, AC-3, AC-6, CM-6, IA-2, IA-4, IA-8, PL-4, PS- 5, PS-6, SC-12, SC-13, SC-17, SC-28.
Control Number	IA-5(1)
Title	Authenticator Management | Password-Based Authentication
DHCS & CDSS Requirement	The information system, for password-based authentication, must: a. Enforces minimum password complexity of requirements for: * case sensitivity (upper and lower case letters), * number of characters (equal to or greater than fifteen characters), * mix of upper-case letters, lower-case letters, numbers, and special characters (at least one of each type);

	c. Stores and transmits only cryptographically-protected passwords; d. Enforces password lifetime of at least 180 days; e. Prohibits prior 10 passwords for reuse; and f. Allows the use of a temporary password for system logons with an immediate change to a permanent password.
Supplemental Guidance (from NIST 800-53)	This control enhancement applies to single-factor authentication of individuals using passwords as individual or group authenticators, and in a similar manner, when passwords are part of multifactor authenticators. This control enhancement does not apply when passwords are used to unlock hardware authenticators (e.g., Personal Identity Verification cards). The implementation of such password mechanisms may not meet all of the requirements in the enhancement. Cryptographically-protected passwords include, for example, encrypted versions of passwords and one-way cryptographic hashes of passwords. The number of changed characters refers to the number of changes required with respect to the total number of positions in the current password. Password lifetime restrictions do not apply to temporary passwords. To mitigate certain brute force attacks against passwords, organizations may also consider salting passwords. Related control: IA-6.

8. **Incident Response (IR)**

Control Number	IR-1
Title	Incident Response Policy and Procedures
DHCS & CDSS Requirement	The organization must: a. Develops, documents, and disseminates to organization-defined personnel or roles: 1. An incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the incident response policy and associated incident response controls; and b. Reviews and updates the current: 1. Incident response policy with organization-defined frequency; and 2. Incident response procedures with organization-defined frequency. *DHCS, CDSS and NIST Guidelines encourage agencies to consider establishing incident response teams or identifying individuals specifically responsible for addressing PII, DHCS* and CDSS *data breaches.*
Supplemental Guidance (from NIST 800-53)	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the IR family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures.

	Related control: PM-9.
Control Number	IR-2
Title	Incident Response Training
DHCS & CDSS Requirement	The organization must provide incident response training to information system users consistent with assigned roles and responsibilities: a. Within organization-defined time period of assuming an incident response role or responsibility; b. When required by information system changes; and c. With organization-defined frequency thereafter.
Supplemental Guidance (from NIST 800-53)	Incident response training provided by organizations is linked to the assigned roles and responsibilities of organizational personnel to ensure the appropriate content and level of detail is included in such training. For example, regular users may only need to know who to call or how to recognize an incident on the information system; system administrators may require additional training on how to handle/remediate incidents; and incident responders may receive more specific training on forensics, reporting, system recovery, and restoration. Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. Related controls: AT-3, CP-3, IR-8.
Control Number	IR-4
Title	Incident Handling
DHCS & CDSS Requirement	The organization must: a. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery; b. Coordinates incident handling activities with contingency planning activities; and c. Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.
Supplemental Guidance (from NIST 800-53)	Organizations recognize that incident response capability is dependent on the capabilities of organizational information systems and the mission/business processes being supported by those systems. Therefore, organizations consider incident response as part of the definition, design, and development of mission/business processes and information systems. Incident- related information can be obtained from a variety of sources including, for example, audit monitoring, network monitoring, physical access monitoring, user/administrator reports, and reported supply chain events. Effective incident handling capability includes coordination among many organizational entities including, for example, mission/business owners, information system owners, authorizing officials, human resources offices, physical and personnel security offices, legal departments, operations personnel, procurement offices, and the risk executive (function). Related controls: AU-6, CM-6, CP-2, CP-4, IR-2, IR-3, IR-8, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.
Control Number	IR-8
Title	Incident Response Plan
DHCS & CDSS Requirement	The organization must: a. Develop an incident response plan that: 1. Provides the organization with a roadmap for implementing its incident response capability; 2. Describes the structure and organization of the incident response capability;

	3. Provides a high-level approach for how the incident response capability fits into the overall organization; 4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions; 5. Defines reportable incidents; 6. Provides metrics for measuring the incident response capability within the organization; 7. Defines the resources and management support needed to effectively maintain and mature an incident response capability; and 8. Is reviewed and approved by organization-defined personnel or roles; b. Distribute copies of the incident response plan to organization-defined incident response personnel (identified by name and/or by role) and organizational elements; c. Review the incident response plan organization-defined frequency; d. Updates the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; e. Communicate incident response plan changes to organization-defined incident response personnel (identified by name and/or by role) and organizational elements]; and f. Protect the incident response plan from unauthorized disclosure and modification.
Supplemental Guidance (from NIST 800-53)	It is important that organizations develop and implement a coordinated approach to incident response. Organizational missions, business functions, strategies, goals, and objectives for incident response help to determine the structure of incident response capabilities. As part of a comprehensive incident response capability, organizations consider the coordination and sharing of information with external organizations, including, for example, external service providers and organizations involved in the supply chain for organizational information systems. Related controls: MP-2, MP-4, MP-5.

9. **Media Protection (MP)**

Control Number	MP-2
Title	Media Access
DHCS & CDSS Requirement	The organization must: Restricts access to PII to Contractor Workers who require access to PII for purposes of administering the Medi-Cal program or as required for the administration of other public benefit programs.
Supplemental Guidance (from NIST 800-53)	Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm. Restricting non-digital media access includes, for example, denying access to patient medical records in a community hospital unless the individuals seeking access to such records are authorized healthcare providers. Restricting access to digital media includes, for example, limiting access to design specifications stored on compact disks in the media library to the project leader and the individuals on the development team. Related controls: AC-3, IA-2, MP-4, PE-2, PE-3, PL-2.
Control Number	MP-6
Title	Media Sanitization

DHCS & CDSS Requirement	The organization must: a. Sanitize media containing PII prior to disposal, release out of organizational control, or release for reuse in accordance with applicable federal and organizational standards and policies; and b. Employs sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.
Supplemental Guidance (from NIST 800-53)	This control applies to all information system media, both digital and non-digital, subject to disposal or reuse, whether or not the media is considered removable. Examples include media found in scanners, copiers, printers, notebook computers, workstations, network components, and mobile devices. The sanitization process removes information from the media such that the information cannot be retrieved or reconstructed. Sanitization techniques, including clearing, purging, cryptographic erase, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused or released for disposal. Organizations determine the appropriate sanitization methods recognizing that destruction is sometimes necessary when other methods cannot be applied to media requiring sanitization. Organizations use discretion on the employment of approved sanitization techniques and procedures for media containing information deemed to be in the public domain or publicly releasable, or deemed to have no adverse impact on organizations or individuals if released for reuse or disposal. Sanitization of non-digital media includes, for example, removing a classified appendix from an otherwise unclassified document, or redacting selected sections or words from a document by obscuring the redacted sections/words in a manner equivalent in effectiveness to removing them from the document. NSA standards and policies control the sanitization process for media containing classified information. Related controls: MA-2, MA-4, RA-3, SC-4.

10. **Personnel Security (PS)**

Control Number	PS-3
Title	Personnel Screening
DHCS & CDSS Requirement	The organization must: a. Screen individuals (employees, contractors and agents) prior to authorizing access to the information system and PII.
Supplemental Guidance (from NIST 800-53)	Personnel screening and rescreening activities reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, guidance, and specific criteria established for the risk designations of assigned positions. Organizations may define different rescreening conditions and frequencies for personnel accessing information systems based on types of information processed, stored, or transmitted by the systems.
Control Number	PS-4
Title	Personnel Termination
DHCS & CDSS Requirement	The organization, upon termination of individual employment, must: a. Disable information system access; b. Terminate/revoke any authenticators/credentials associated with the individual; c. Conduct exit interviews, as needed; d. Retrieve all security-related organizational information system-related property; e. Retain access to organizational information and information systems formerly controlled by

	terminated individual; and f. Notified organization-defined personnel upon termination.
Supplemental Guidance (from NIST 800-53)	Information system-related property includes, for example, hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews ensure that terminated individuals understand the security constraints imposed by being former employees and that proper accountability is achieved for information system-related property. Security topics of interest at exit interviews can include, for example, reminding terminated individuals of nondisclosure agreements and potential limitations on future employment. Exit interviews may not be possible for some terminated individuals, for example, in cases related to job abandonment, illnesses, and non-availability of supervisors. Exit interviews are important for individuals with security clearances. Timely execution of termination actions is essential for individuals terminated for cause. In certain situations, organizations consider disabling the information system accounts of individuals that are being terminated prior to the individuals being notified. Related controls: AC-2, IA-4, PE-2, PS-5, PS-6.
Control Number	PS-6
Title	Access Agreements
DHCS & CDSS Requirement	The organization must: a. Develop and document access agreements for organizational information systems; b. Reviews and updates the access agreements at organization-defined frequency; and c. Ensure that individuals requiring access to organizational information and information systems: 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational information systems when access agreements have been updated or at an organization-defined frequency. DHCS and CDSS requires that contracts for periodic disposal/destruction of case files or other print media contain a non-disclosure agreement signed by all personnel who will encounter products that contain PII.
Supplemental Guidance (from NIST 800-53)	Supplemental Guidance: Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with organizational information systems to which access is authorized. Organizations can use electronic signatures to acknowledge access agreements unless specifically prohibited by organizational policy. Related control: PL-4, PS-2, PS-3, PS-4, PS-8.
Control Number	PS-7
Title	Third-Party Personnel Security
DHCS & CDSS Requirement	The organization must: a. Establishes personnel security requirements including security roles and responsibilities for county agents, subcontractors, and vendors; b. Requires third-party providers to comply with personnel security policies and procedures established by the organization; c. Documents personnel security requirements; d. Requires third-party providers to notify organization-defined personnel or roles of any personnel transfers or terminations of third-party personnel who possess organizational

	credentials and/or badges, or who have information system privileges within organization-defined time period; and e. Monitors provider compliance. *The service level agreements with the contractors and agents must contain non-disclosure language as it pertains to PII. The statement shall include, at a minimum, a description of the following:* *1. General Use of PII;* *2. Security and Privacy Safeguards for PII;* *3. Unacceptable Use of PII; and* *4. Enforcement Policies.* *The county department/agency must retain the non-disclosure agreements for at least five (5) to seven (7) years for all contractors and agents who processes, views, or encounters PII as part of their duties*
Supplemental Guidance (from NIST 800-53)	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. Organizations explicitly include personnel security requirements in acquisition-related documents. Third-party providers may have personnel working at organizational facilities with credentials, badges, or information system privileges issued by organizations. Notifications of third-party personnel changes ensure appropriate termination of privileges and credentials. Organizations define the transfers and terminations deemed reportable by security-related characteristics that include, for example, functions, roles, and nature of credentials/privileges associated with individuals transferred or terminated. Related controls: PS-2, PS-3, PS-4, PS-5, PS-6, SA-9, SA-21.
Control Number	PS-8
Title	Personnel Sanctions
DHCS & CDSS Requirement	The organization must: a. Employ a formal sanctions process for individuals failing to comply with established information security policies and procedures; and b. Notify organization personnel within the organization-defined time period when a formal employee sanctions process is initiated, identifying the individual sanctioned and the reason for the sanction. *If a member of the county's workforce, as defined at 45 CFR 160.103 and inclusive of an employee, contractor, or agent is subject to an adverse action by the organization (e.g., reduction in pay, disciplinary action, termination of employment, termination of contract for services), DHCS and CDSS recommends the organization remove his or her access to PII in advance of the adverse action to reduce the possibility that will the individual will perform unauthorized activities that involve PII, if applicable.*
Supplemental Guidance (from NIST 800-53)	Organizational sanctions processes reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Sanctions processes are described in access agreements and can be included as part of general personnel policies and procedures for organizations. Organizations consult with the Office of the General Counsel regarding matters of employee sanctions. Related controls: PL-4, PS-6.

11. Physical and Environmental Protection (PE)

Control Number	PE-3
Title	Physical Access Control
DHCS & CDSS Requirement	The organization must: a. Enforce physical access authorizations at entry and exit points to the facility where the information system resides by; 1. Verifying individual access authorizations before granting access to the facility; and 2. Controlling ingress/egress to the facility using physical access control systems/devices and/or guards; b. Maintain physical access audit logs for entry and exit points; c. Provide security safeguards to control access to areas within the facility officially designated as publicly accessible; d. Escort visitors and monitors visitor activity; e. Secure keys, combinations, and other physical access devices; f. Inventory physical access devices; and g. Changes combinations and keys at minimum when keys are lost, combinations are compromised, or individuals are transferred or terminated
Supplemental Guidance (from NIST 800-53)	This control applies to organizational employees and visitors. Individuals (e.g., employees, contractors, and others) with permanent physical access authorization credentials are not considered visitors. Organizations determine the types of facility guards needed including, for example, professional physical security staff or other personnel such as administrative staff or information system users. Physical access devices include, for example, keys, locks, combinations, and card readers. Safeguards for publicly accessible areas within organizational facilities include, for example, cameras, monitoring by guards, and isolating selected information systems and/or system components in secured areas. Physical access control systems comply with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance. The Federal Identity, Credential, and Access Management Program provides implementation guidance for identity, credential, and access management capabilities for physical access control systems. Organizations have flexibility in the types of audit logs employed. Audit logs can be procedural (e.g., a written log of individuals accessing the facility and when such access occurred), automated (e.g., capturing ID provided by a PIV card), or some combination thereof. Physical access points can include facility access points, interior access points to information systems and/or components requiring supplemental access controls, or both. Components of organizational information systems (e.g., workstations, terminals) may be located in areas designated as publicly accessible with organizations safeguarding access to such devices. Related controls: AU-2, AU-6, MP-2, MP-4, PE-2, PE-4, PE-5, PS-3, RA-3.
Control Number	PE-6
Title	Monitoring Physical Access
DHCS & CDSS Requirement	The organization must: a. Monitors physical access to the facility where the information system resides to detect and respond to physical security incidents; b. Reviews physical access logs organization-defined frequency and upon occurrence of security incidents; and

	c. Coordinates results of reviews and investigations with the organizational incident response capability.
Supplemental Guidance (from NIST 800-53)	Organizational incident response capabilities include investigations of and responses to detected physical security incidents. Security incidents include, for example, apparent security violations or suspicious physical access activities. Suspicious physical access activities include, for example: (i) accesses outside of normal work hours; (ii) repeated accesses to areas not normally accessed; (iii) accesses for unusual lengths of time; and (iv) out-of-sequence accesses. Related controls: CA-7, IR-4, IR-8.

12. **Planning (PL)**

Control Number	PL-1
Title	Security Planning Policy and Procedures
DHCS & CDSS Requirement	The organization must: a. Develop, document, and disseminate to personnel and organizations with access to PII: 1. A security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the security planning policy and associated security planning controls; and b. Reviews and updates the current: 1. Security planning policy; and 2. Security planning procedures.
Supplemental Guidance (from NIST 800-53)	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the PL family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.
Control Number	PL-2
Title	System Security Plan
DHCS & CDSS Requirement	The organization must: a. Develop a security plan for the information system that: 1. Is consistent with the organization's enterprise architecture; 2. Explicitly defines the authorization boundary for the system; 3. Describes the operational context of the information system in terms of missions and business processes; 4. Provides the security categorization of the information system including supporting

	rationale; 5. Describes the operational environment for the information system and relationships with or connections to other information systems; 6. Provides an overview of the security requirements for the system; 7. Identifies any relevant overlays, if applicable; 8. Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring decisions; and 9. Is reviewed and approved by the authorizing official or designated representative prior to plan implementation; b. Distribute copies of the security plan and communicates subsequent changes to the plan to personnel and organizations with security responsibilities; c. Review the security plan for the information system; d. Update the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments; and e. Protect the security plan from unauthorized disclosure and modification. *Organization's security plan should include detailed information specific to safeguarding Medi- Cal PII.*
Supplemental Guidance (from NIST 800-53)	Security plans relate security requirements to a set of security controls and control enhancements. Security plans also describe, at a high level, how the security controls and control enhancements meet those security requirements, but do not provide detailed, technical descriptions of the specific design or implementation of the controls/enhancements. Security plans contain sufficient information (including the specification of parameter values for assignment and selection statements either explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended. Organizations can also apply tailoring guidance to the security control baselines in Appendix D and CNSS Instruction 1253 to develop overlays for community-wide use or to address specialized requirements, technologies, or missions/environments of operation (e.g., DoD-tactical, Federal Public Key Infrastructure, or Federal Identity, Credential, and Access Management, space operations). Appendix I provides guidance on developing overlays. Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained. This reduces the documentation requirements associated with security programs and maintains security-related information in other established management/operational areas related to enterprise architecture, system development life cycle, systems engineering, and acquisition. For example, security plans do not contain detailed contingency plan or incident response plan information but instead provide explicitly or by reference, sufficient information to define what needs to be accomplished by those plans. Related controls: AC-2, AC-6, AC-14, AC-17, AC-20, CA-2, CA-3, CA-7, CM-9, CP-2, IR-8, MA-4, MA-5, MP-2, MP-4, MP-5, PL-7, PM-1, PM-7, PM-8, PM-9, PM-11, SA-5, SA- 17.

13. **Risk Assessment (RA)**

Control Number	RA-1
Title	Risk Assessment Policy and Procedures

DHCS & CDSS Requirement	The organization must: a. Develop, document, and disseminate to system owners using PII: 1. A risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and 2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls.
Supplemental Guidance (from NIST 800-53)	This control addresses the establishment of policy and procedures for the effective implementation of selected security controls and control enhancements in the RA family. Policy and procedures reflect applicable federal laws, Executive Orders, directives, regulations, policies, standards, and guidance. Security program policies and procedures at the organization level may make the need for system-specific policies and procedures unnecessary. The policy can be included as part of the general information security policy for organizations or conversely, can be represented by multiple policies reflecting the complex nature of certain organizations. The procedures can be established for the security program in general and for particular information systems, if needed. The organizational risk management strategy is a key factor in establishing policy and procedures. Related control: PM-9.
Control Number	RA-3
Title	Risk Assessment
DHCS & CDSS Requirement	The organization must: a. Conduct 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; b. Documents risk assessment results in a risk assessment report or organization defined risk report document. c. Review risk assessment results annually; and e. Update the risk assessment whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.
Supplemental Guidance (from NIST 800-53)	Clearly defined authorization boundaries are a prerequisite for effective risk assessments. Risk assessments take into account threats, vulnerabilities, likelihood, and impact to organizational operations and assets, individuals, other organizations, and the Nation based on the operation and use of information systems. Risk assessments also take into account risk from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities). In accordance with OMB policy and related E-authentication initiatives, authentication of public users accessing federal information systems may also be required to protect nonpublic or privacy-related information. As such, organizational assessments of risk also address public access to federal information systems. Risk assessments (either formal or informal) can be conducted at all three tiers in the risk management hierarchy (i.e., organization level, mission/business process level, or information system level) and at any phase in the system development life cycle. Risk assessments can also be conducted at various steps in the Risk Management Framework, including categorization, security control selection, security control implementation, security control assessment, information system authorization, and security control monitoring. RA-3 is noteworthy in that the control must be partially implemented prior to the implementation of other controls in order to complete the first two steps in the Risk Management Framework. Risk assessments can play an important role in security control selection processes, particularly during the application of tailoring guidance, which

	includes security control supplementation. Related controls: RA-2, PM- 9.
Control Number	RA-5
Title	Vulnerability Scanning
DHCS & CDSS Requirement	The organization must: a. Scan for vulnerabilities in the information system and hosted applications at a minimum of a monthly basis 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: 1. Enumerating platforms, software flaws, and improper configurations; a. Analyze vulnerability scan reports and results from security control assessments; b. Remediate legitimate vulnerabilities within organization defined time periods in accordance with an organizational assessment of risk; and c. Share information obtained from the vulnerability scanning process and security control assessments with all impacted system owners to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).
Supplemental Guidance (from NIST 800-53)	Security categorization of information systems guides the frequency and comprehensiveness of vulnerability scans. Organizations determine the required vulnerability scanning for all information system components, ensuring that potential sources of vulnerabilities such as networked printers, scanners, and copiers are not overlooked. Vulnerability analyses for custom software applications may require additional approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Organizations can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Vulnerability scanning includes, for example: (i) scanning for patch levels; (ii) scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and (iii) scanning for improperly configured or incorrectly operating information flow control mechanisms. Organizations consider using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to determine/test for the presence of vulnerabilities. Suggested sources for vulnerability information include the Common Weakness Enumeration (CWE) listing and the National Vulnerability Database (NVD). In addition, security control assessments such as red team exercises provide other sources of potential vulnerabilities for which to scan. Organizations also consider using tools that express vulnerability impact by the Common Vulnerability Scoring System (CVSS). Related controls: CA-2, CA-7, CM-4, CM-6, RA- 2, RA-3, SA-11, SI-2.

14. **Security Assessment and Authorization (CA)**

Control Number	CA-2
Title	Security Assessments
DHCS & CDSS Requirement	The organization must: a. Develops a security assessment plan that describes the scope of the assessment including: 1. Security controls and control enhancements under assessment; 2. Assessment procedures to be used to determine security control effectiveness; and

	3. Assessment environment, assessment team, and assessment roles and responsibilities; b. Assesses the security controls in the information system and its environment of operation wit organization-defined frequency to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; c. Produces a security assessment report that documents the results of the assessment; and d. Provides the results of the security control assessment to organization-defined individuals or roles.
Supplemental Guidance (from NIST 800-53)	Organizations assess security controls in organizational information systems and the environments in which those systems operate as part of: (i) initial and ongoing security authorizations; (ii) FISMA annual assessments; (iii) continuous monitoring; and (iv) system development life cycle activities. Security assessments: (i) ensure that information security is built into organizational information systems; (ii) identify weaknesses and deficiencies early in the development process; (iii) provide essential information needed to make risk-based decisions as part of security authorization processes; and (iv) ensure compliance to vulnerability mitigation procedures. Assessments are conducted on the implemented security controls from Appendix F (main catalog) and Appendix G (Program Management controls) as documented in System Security Plans and Information Security Program Plans. Organizations can use other types of assessment activities such as vulnerability scanning and system monitoring to maintain the security posture of information systems during the entire life cycle. Security assessment reports document assessment results in sufficient detail as deemed necessary by organizations, to determine the accuracy and completeness of the reports and whether the security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements. The FISMA requirement for assessing security controls at least annually does not require additional assessment activities to those activities already in place in organizational security authorization processes. Security assessment results are provided to the individuals or roles appropriate for the types of assessments being conducted. For example, assessments conducted in support of security authorization decisions are provided to authorizing officials or authorizing official designated representatives. To satisfy annual assessment requirements, organizations can use assessment results from the following sources: (i) initial or ongoing information system authorizations; (ii) continuous monitoring; or (iii) system development life cycle activities. Organizations ensure that security assessment results are current, relevant to the determination of security control effectiveness, and obtained with the appropriate level of assessor independence. Existing security control assessment results can be reused to the extent that the results are still valid and can also be supplemented with additional assessments as needed. Subsequent to initial authorizations and in accordance with OMB policy, organizations assess security controls during continuous monitoring. Organizations establish the frequency for ongoing security control assessments in accordance with organizational continuous monitoring strategies. Information Assurance Vulnerability Alerts provide useful examples of vulnerability mitigation procedures. External audits (e.g., audits by external entities such as regulatory agencies) are outside the scope of this control. Related controls: CA-5, CA-6, CA-7, PM-9, RA-5, SA-11, SA-12, SI-4.
Control Number	CA-3
Title	System Interconnections
DHCS & CDSS Requirement	The organization must: a. Authorizes connections from the information system to other information systems through the

	use of Interconnection Security Agreements; b. Documents, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and c. Reviews and updates Interconnection Security Agreements [Assignment: organization-defined frequency].
Supplemental Guidance (from NIST 800-53)	This control applies to dedicated connections between information systems (i.e., system interconnections) and does not apply to transitory, user-controlled connections such as email and website browsing. Organizations carefully consider the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within organizations and external to organizations. Authorizing officials determine the risk associated with information system connections and the appropriate controls employed. If interconnecting systems have the same authorizing official, organizations do not need to develop Interconnection Security Agreements. Instead, organizations can describe the interface characteristics between those interconnecting systems in their respective security plans. If interconnecting systems have different authorizing officials within the same organization, organizations can either develop Interconnection Security Agreements or describe the interface characteristics between systems in the security plans for the respective systems. Organizations may also incorporate Interconnection Security Agreement information into formal contracts, especially for interconnections established between federal agencies and nonfederal (i.e., private sector) organizations. Risk considerations also include information systems sharing the same networks. For certain technologies (e.g., space, unmanned aerial vehicles, and medical devices), there may be specialized connections in place during preoperational testing. Such connections may require Interconnection Security Agreements and be subject to additional security controls. Related controls: AC-3, AC-4, AC-20, AU-2, AU-12, AU-16, CA-7, IA-3, SA-9, SC-7, SI-4.
Control Number	CA-7
Title	Continuous Monitoring
DHCS & CDSS Requirement	The organization must develop a continuous monitoring strategy and implement a continuous monitoring program that includes: a. Establishment of PII security controls to be monitored; c. Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; d. Ongoing security status monitoring of PII security controls in accordance with the organizational continuous monitoring strategy; e. Correlation and analysis of security-related information generated by assessments and monitoring; f. Response actions to address results of the analysis of security-related information; and g. Reporting the security status of organization and the information system to organization-defined personnel or roles and to DHCS and CDSS when requested.
Supplemental Guidance (from NIST 800-53)	Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess/analyze security controls and information security- related risks at a frequency sufficient to support organizational risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Continuous monitoring programs also allow organizations to maintain the security authorizations of information systems and common controls over time in highly dynamic environments of operation

	with changing mission/business needs, threats, vulnerabilities, and technologies. Having access to security-related information on a continuing basis through reports/dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions. Automation supports more frequent updates to security authorization packages, hardware/software/firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of information systems. Related controls: CA-2, CA-5, CA-6, CM-3, CM-4, PM-6, PM-9, RA-5, SA- 11, SA-12, SI-2, SI-4.
Control Number	CA-8
Title	Penetration Testing
DHCS & CDSS Requirement	The organization must conduct penetration testing annually on systems storing, processing, or transmitting PII.
Supplemental Guidance (from NIST 800-53)	Penetration testing is a specialized type of assessment conducted on information systems or individual system components to identify vulnerabilities that could be exploited by adversaries. Such testing can be used to either validate vulnerabilities or determine the degree of resistance organizational information systems have to adversaries within a set of specified constraints (e.g., time, resources, and/or skills). Penetration testing attempts to duplicate the actions of adversaries in carrying out hostile cyber-attacks against organizations and provides a more in- depth analysis of security-related weaknesses/deficiencies. Organizations can also use the results of vulnerability analyses to support penetration testing activities. Penetration testing can be conducted on the hardware, software, or firmware components of an information system and can exercise both physical and technical security controls. A standard method for penetration testing includes, for example: (i) pretest analysis based on full knowledge of the target system; (ii) pretest identification of potential vulnerabilities based on pretest analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. All parties agree to the rules of engagement before the commencement of penetration testing scenarios. Organizations correlate the penetration testing rules of engagement with the tools, techniques, and procedures that are anticipated to be employed by adversaries carrying out attacks. Organizational risk assessments guide decisions on the level of independence required for personnel conducting penetration testing. Related control: SA-12.

15. **System and Communications Protection (SC)**

Control Number	SC-7
Title	Boundary Protection
DHCS & CDSS Requirement	The organization information system must: a. Monitor and control communications at the external boundary of the system and at key internal boundaries within the system; b. Implements subnetworks for publicly accessible system components that are physically and logically separated from internal organizational networks; and c. Connect to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

Supplemental Guidance (from NIST 800-53)	Managed interfaces include, for example, gateways, routers, firewalls, guards, network-based malicious code analysis and virtualization systems, or encrypted tunnels implemented within a security architecture (e.g., routers protecting firewalls or application gateways residing on protected subnetworks). Subnetworks that are physically or logically separated from internal networks are referred to as demilitarized zones or DMZs. Restricting or prohibiting interfaces within organizational information systems includes, for example, restricting external web traffic to designated web servers within managed interfaces and prohibiting external traffic that appears to be spoofing internal addresses. Organizations consider the shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may also include third party-provided access lines and other service elements. Such transmission services may represent sources of increased risk despite contract security provisions. Related controls: AC-4, AC-17, CA-3, CM-7, CP-8, IR-4, RA-3, SC-5, SC-13.
Control Number	SC-8
Title	Transmission Confidentiality and Integrity
DHCS & CDSS Requirement	The organization information system must: Protect the confidentiality of transmitted information.
Supplemental Guidance (from NIST 800-53)	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). Communication paths outside the physical protection of a controlled boundary are exposed to the possibility of interception and modification. Protecting the confidentiality and/or integrity of organizational information can be accomplished by physical means (e.g., by employing protected distribution systems) or by logical means (e.g., employing encryption techniques). Organizations relying on commercial providers offering transmission services as commodity services rather than as fully dedicated services (i.e., services which can be highly specialized to individual customer needs), may find it difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality/integrity. In such situations, organizations determine what types of confidentiality/integrity services are available in standard, commercial telecommunication service packages. If it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, organizations implement appropriate compensating security controls or explicitly accept the additional risk. Related controls: AC-17, PE-4.
Control Number	SC-8(1)
Title	Transmission Confidentiality and Integrity | Cryptographic or Alternate Physical Protection
DHCS & CDSS Requirement	The organization information system must implement cryptographic mechanisms to prevent unauthorized disclosure of information during transmission.
Supplemental Guidance (from NIST 800-53)	Encrypting information for transmission protects information from unauthorized disclosure and modification. Cryptographic mechanisms implemented to protect information integrity include, for example, cryptographic hash functions which have common application in digital signatures, checksums, and message authentication codes. Alternative physical security safeguards include, for example, protected distribution systems. Related control: SC-13.
Control Number	Control Number SC-13

SC-13	
Title	Cryptographic Protection
CDSS Requirement	The organization information system must implement FIPS 140-3 compliant encryption modules in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.
Supplemental Guidance (from NIST 800-53)	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. Cryptography can also be used to support random number generation and hash generation. Generally applicable cryptographic standards include FIPS-validated cryptography and NSA-approved cryptography. This control does not impose any requirements on organizations to use cryptography. However, if cryptography is required based on the selection of other security controls, organizations define each type of cryptographic use and the type of cryptography required (e.g., protection of classified information: NSA-approved cryptography; provision of digital signatures: FIPS-validated cryptography). Related controls: AC-2, AC-3, AC-7, AC-17, AC- 18, AU-9, AU-10, CM-11, CP-9, IA-3, IA-7, MA-4, MP-2, MP-4, MP-5, SA-4, SC-8, SC-12, SC-28, SI-7.
Control Number	SC-28
Title	Protection of Information at Rest
DHCS & CDSS Requirement	The organization information system must: Protect the confidentiality of PII at rest.
Supplemental Guidance (from NIST 800-53)	This control addresses the confidentiality and integrity of information at rest and covers user information and system information. Information at rest refers to the state of information when it is located on storage devices as specific components of information systems. System-related information requiring protection includes, for example, configurations or rule sets for firewalls, gateways, intrusion detection/prevention systems, filtering routers, and authenticator content. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning. Integrity protection can be achieved, for example, by implementing Write-Once-Read-Many (WORM) technologies. Organizations may also employ other security controls including, for example, secure off-line storage in lieu of online storage when adequate protection of information at rest cannot otherwise be achieved and/or continuous monitoring to identify malicious code at rest. Related controls: AC-3, AC-6, CA-7, CM-3, CM-5, CM-6, PE-3, SC-8, SC-13, SI-3, SI-7.

16. **System and Information Integrity (SI)**

Control Number	SI-2
Title	Flaw Remediation
DHCS & CDSS Requirement	The organization must: a. Identify, report, and correct information system flaws; b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; c. Installs security-relevant software and firmware updates, within acceptable organization standards, of the release of the updates; and

	d. Incorporates flaw remediation into the organizational configuration management process.
Supplemental Guidance (from NIST 800-53)	Organizations identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures. Organizations also address flaws discovered during security assessments, continuous monitoring, incident response activities, and system error handling. Organizations take advantage of available resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By incorporating flaw remediation into ongoing configuration management processes, required/anticipated remediation actions can be tracked and verified. Flaw remediation actions that can be tracked and verified include, for example, determining whether organizations follow US-CERT guidance and Information Assurance Vulnerability Alerts. Organization-defined time periods for updating security-relevant software and firmware may vary based on a variety of factors including, for example, the security category of the information system or the criticality of the update (i.e., severity of the vulnerability related to the discovered flaw). Some types of flaw remediation may require more testing than other types. Organizations determine the degree and type of testing needed for the specific type of flaw remediation activity under consideration and also the types of changes that are to be configuration-managed. In some situations, organizations may determine that the testing of software and/or firmware updates is not necessary or practical, for example, when implementing simple anti-virus signature updates. Organizations may also consider in testing decisions, whether security- relevant software or firmware updates are obtained from authorized sources with appropriate digital signatures. Related controls: CA-2, CA-7, CM-3, CM-5, CM-8, MA-2, IR-4, RA-5, SA-10, SA-11, SI-11.
Control Number	SI-3
Title	Malicious Code Protection
DHCS & CDSS Requirement	The organization must: 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 organizational configuration management policy and procedures; c. Configure malicious code protection mechanisms to: 1. Perform periodic scans of the information system and real-time scans of files from external sources at the endpoint and network entry/exit points as the files are downloaded, opened, or executed in accordance with organizational security policy; and 2. Block malicious code or quarantine malicious code, and send alert to administrator for incident handling in response to malicious code detection; and d. Address the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system
Supplemental Guidance (from NIST 800-53)	Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, remote-access servers, workstations, notebook computers, and mobile devices. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode), contained within compressed or hidden files, or hidden in files using steganography. Malicious code can be transported by different means including, for example, web accesses, electronic mail, electronic mail attachments,

	and portable storage devices. Malicious code insertions occur through the exploitation of information system vulnerabilities. Malicious code protection mechanisms include, for example, anti-virus signature definitions and reputation-based technologies. A variety of technologies and methods exist to limit or eliminate the effects of malicious code. Pervasive configuration management and comprehensive software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions/business functions. Traditional malicious code protection mechanisms cannot always detect such code. In these situations, organizations rely instead on other safeguards including, for example, secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to help ensure that software does not perform functions other than the functions intended. Organizations may determine that in response to the detection of malicious code, different actions may be warranted. For example, organizations can define actions in response to malicious code detection during periodic scans, actions in response to detection of malicious downloads, and/or actions in response to detection of maliciousness when attempting to open or execute files. Related controls: CM-3, MP-2, SA-4, SA-8, SA-12, SA-13, SC-7, SC-26, SC-44, SI-2, SI-4, SI-7.
Control Number	SI-4
Title	Information System Monitoring
DHCS & CDSS Requirement	The organization must: a. Monitor the information system to detect: 1. Attacks and indicators of potential attacks in accordance with organization-defined monitoring objectives; and 2. Unauthorized local, network, and remote connections; b. Identify unauthorized use of the information system through organization-defined techniques and methods; c. Deploy monitoring devices: 1. Strategically within the information system to collect organization-determined essential information; and 2. At ad hoc locations within the system to track specific types of transactions of interest to the organization; 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 organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; Relevant risk would apply to anything impacting the confidentiality integrity or availability of the information system. f. Obtain legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and g. Provides organization-defined information system monitoring information to organization-defined personnel and DHCS and CDSS as needed.
Supplemental Guidance (from	Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the information system boundary (i.e., part of perimeter

NIST 800-53)	defense and boundary protection). Internal monitoring includes the observation of events occurring within the information system. Organizations can monitor information systems, for example, by observing audit activities in real time or by observing other system aspects such as access patterns, characteristics of access, and other actions. The monitoring objectives may guide determination of the events. Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, scanning tools, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. Einstein network monitoring devices from the Department of Homeland Security can also be included as monitoring devices. The granularity of monitoring information collected is based on organizational monitoring objectives and the capability of information systems to support such objectives. Specific types of transactions of interest include, for example, Hyper Text Transfer Protocol (HTTP) traffic that bypasses HTTP proxies. Information system monitoring is an integral part of organizational continuous monitoring and incident response programs. Output from system monitoring serves as input to continuous monitoring and incident response programs. A network connection is any connection with a device that communicates through a network (e.g., local area network, Internet). A remote connection is any connection with a device communicating through an external network (e.g., the Internet). Local, network, and remote connections can be either wired or wireless. Related controls: AC-3, AC-4, AC-8, AC-17, AU-2, AU-6, AU-7, AU-9, AU-12, CA-7, IR-4, PE-3, RA-5, SC-7, SC-26, SC-35, SI-3, SI-7.
Control Number	SI-4(5)
Title	Information System Monitoring | System Generated Alerts
DHCS & CDSS Requirement	The information system alerts County Worker when the following indications of compromise or potential compromise occur. County will notify Contractor as needed. 1. Protected system files or directories have been modified without notification from the appropriate change/configuration management channels. 2. System performance indicates resource consumption that is inconsistent with expected operating conditions. 3. Auditing functionality has been disabled or modified to reduce audit visibility. 4. Audit or log records have been deleted or modified without explanation. 5. The system is raising alerts or faults in a manner that indicates the presence of an abnormal condition. 6. Resource or service requests are initiated from clients that are outside of the expected client membership set. 7. The system reports failed logins or password changes for administrative or key service accounts. 8. Processes and services are running that are outside of the baseline system profile. 9. Utilities, tools, or scripts have been saved or installed on production systems without clear indication of their use or purpose.
Supplemental Guidance (from NIST 800-53)	Alerts 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. Alerts can be transmitted, for example, telephonically, by electronic mail messages, or by text messaging. Organizational personnel on the notification list can include, for example, system administrators, mission/business owners, system

	owners, or information system security officers. Related controls: AU-5, PE-6.
Control Number	SI-4(13)
Title	Information System Monitoring | Analyze Traffic / Event Patterns
DHCS & CDSS Requirement	The organization must: a. Analyzes communications traffic/event patterns for the information system; b. Develops profiles representing common traffic patterns and/or events; and c. Uses the traffic/event profiles in tuning system-monitoring devices to reduce the number of false positives and the number of false negatives.
Supplemental Guidance (from NIST 800-53)	None

17. **System and Services Acquisition (SA)**

Control Number	**SA-9**
Title	External Information System Services
DHCS & CDSS Requirement	The organization must: a. Require that providers of external information system services comply with organizational information security requirements and employ organization-defined security controls in accordance with DHCS and CDSS PSA, applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; b. Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and c. Employs organization-defined processes, methods, and techniques to monitor security control compliance by external service providers on an ongoing basis. *The state organization will provide its contractors and agents with copies of the Agreement, related IEAs, and all related attachments before initial disclosure of PII to such contractors and agents. Prior to signing the Agreement, and thereafter at DHCS's and CDSS's request, the state organization will obtain from its contractors and agents a current list of the employees of such contractors and agents with access to PII and provide such lists to DHCS and CDSS.*
Supplemental Guidance (from NIST 800-53)	External information system services are services that are implemented outside of the authorization boundaries of organizational information systems. This includes services that are used by, but not a part of, organizational information systems. FISMA and OMB policy require that organizations using external service providers that are processing, storing, or transmitting federal information or operating information systems on behalf of the federal government ensure that such providers meet the same security requirements that federal agencies are required to meet. Organizations establish relationships with external service providers in a variety of ways including, for example, through joint ventures, business partnerships, contracts, interagency agreements, lines of business arrangements, licensing agreements, and supply chain exchanges. The responsibility for managing risks from the use of external information system services remains with authorizing officials. For services external to organizations, a chain of trust requires that organizations establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered. The extent and nature of this chain of trust varies based on the relationships between organizations and the external providers. Organizations document the basis for

	trust relationships so the relationships can be monitored over time. External information system services documentation includes government, service providers, end user security roles and responsibilities, and service-level agreements. Service-level agreements define expectations of performance for security controls, describe measurable outcomes, and identify remedies and response requirements for identified instances of noncompliance. Related controls: CA-3, IR-7, PS-7.
Control Number	SA-11
Title	Developer Security Testing And Evaluation
DHCS & CDSS Requirement	The organization must require the developer of the information system, system component, or information system service to: a. Create and implement a security assessment plan; b. Perform [Selection (one or more): unit; integration; system; regression] testing/evaluation at [Assignment: organization-defined depth and coverage]; c. Produce evidence of the execution of the security assessment plan and the results of the security testing/evaluation; d. Implement a verifiable flaw remediation process; and e. Correct flaws identified during security testing/evaluation
Supplemental Guidance (from NIST 800-53)	Supplemental Guidance: Developmental security testing/evaluation occurs at all post-design phases of the system development life cycle. Such testing/evaluation confirms that the required security controls are implemented correctly, operating as intended, enforcing the desired security policy, and meeting established security requirements. Security properties of information systems may be affected by the interconnection of system components or changes to those components. These interconnections or changes (e.g., upgrading or replacing applications and operating systems) may adversely affect previously implemented security controls. This control provides additional types of security testing/evaluation that developers can conduct to reduce or eliminate potential flaws. Testing custom software applications may require approaches such as static analysis, dynamic analysis, binary analysis, or a hybrid of the three approaches. Developers can employ these analysis approaches in a variety of tools (e.g., web-based application scanners, static analysis tools, binary analyzers) and in source code reviews. Security assessment plans provide the specific activities that developers plan to carry out including the types of analyses, testing, evaluation, and reviews of software and firmware components, the degree of rigor to be applied, and the types of artifacts produced during those processes. The depth of security testing/evaluation refers to the rigor and level of detail associated with the assessment process (e.g., black box, gray box, or white box testing). The coverage of security testing/evaluation refers to the scope (i.e., number and type) of the artifacts included in the assessment process. Contracts specify the acceptance criteria for security assessment plans, flaw remediation processes, and the evidence that the plans/processes have been diligently applied. Methods for reviewing and protecting assessment plans, evidence, and documentation are commensurate with the security category or classification level of the information system. Contracts may specify documentation protection requirements. Related controls: CA-2, CM-4, SA-3, SA-4, SA-5, SI-2.

[Remainder of page intentionally left blank]

B. ***Minimum Cloud Security Requirements***

Contractor and any agents, subcontractors, and vendors storing PII in a cloud service must comply with the Cloud Computing Policy, State Administration Manual (SAM) Sections 4983-4983.1, and employ the capabilities in the Cloud Security Standard, SIMM 5315-B to protect information and systems in cloud services as outlined below.

1. Identify and classify assets to focus and prioritize efforts in aligning business needs and risk management.

2. Each information asset for which the Contractor entity has ownership responsibility shall be inventoried and identified to include the following:

    a. Description and value of the information asset.
    b. Owner of the information asset.
    c. Custodians of the information asset.
    d. Users of the information asset.
    e. Classification of information.
    f. FIPS Publication 199 categorization and level of protection (Low, Moderate, or High).
    g. Importance of information assets to the execution of the Agency/state entity's mission and program function.
    h. Potential consequences and impacts if confidentiality, integrity, and availability of the information asset were compromised.

3. Security of cloud services stems from managing authentication and fine- grained authorization. To safeguard cloud systems, Contractor shall establish processes and procedures to ensure:

    a. Maintenance of user identities, including both provisioning and de- provisioning;
    b. Enforcement of password policies or more advanced multifactor mechanisms to authenticate users and devices;
    c. Management of access control rules, limiting access to the minimum necessary to complete defined responsibilities;
    d. Separation of duties to avoid functional conflicts;
    e. Periodic recertification of access control rules to identify those that are no longer needed or provide overly broad clearance;
    f. Use of privileged accounts that can bypass security are restricted and audited;
    g. Systems to administer access based on roles are defined and installed; and
    h. Encryption keys and system security certificates are effectively generated, exchanged, stored and safeguarded.

4. Infrastructure protection controls limit the impact of unintended access or potential vulnerabilities. PaaS and SaaS resources may already have these controls implemented by the service provider. Contractor must configure information assets to provide only essential capabilities.

5. Contractor is entrusted with protecting the integrity and confidentiality of data processed by their information systems. Cloud technologies simplify data protection by providing managed

data storage services with native protection and backup features, but these features must be configured and managed appropriately.

6. Detective controls identify potential security threats or incidents, supporting timely investigation and response. Contractor must continuously identify and remediate vulnerabilities.

7. Response controls enable timely event and incident response which is essential to reducing the impact if an incident were to occur. Compliance with incident management requirements as outlined in VII. Notification and Investigation of Breaches and Security Incidents.

8. Recover controls facilitate long-term recovery activities following events or incidents. With cloud services, primarily SaaS solutions, the services provider hosts the data in its application, and unless properly planned and provisioned for in the contract with the service provider it may be difficult or impossible to obtain the data in a usable format at contract termination. Contractor must ensure agreements with cloud service providers include recover controls.

C. ***Minimum Necessary.*** Only the minimum necessary amount of PII required to perform required business functions applicable to the terms of this Agreement may be used, disclosed, copied, downloaded, or exported.

D. ***Transmission and Storage of PII.*** All persons that will be working with PII shall employ FIPS 140-2 or greater approved security functions as described in section 6.2.2 of NIST SP 800-140Cr1 encryption of PII at rest and in motion unless Contractor determines it is not reasonable and appropriate to do so based upon a risk assessment, and equivalent alternative measures are in place and documented as such. In addition, Contractor shall maintain, at a minimum, the most current industry standards for transmission and storage of County of Orange data and other confidential information.

E. ***DHCS Remote Work Policy.*** Contractor, its Contractor Workers and any agents, subcontractors, and vendors accessing PII pursuant to this PSA when working remotely, shall follow reasonable policies and procedures that are equivalent to or better than the DHCS Remote Work Policy, as published in Medi-Cal Eligibility Division Informational Letter (MEDIL) | 23-35E. Working remotely means working from a physical location not under the control of the person's employer.

If DHCS changes the terms of the DHCS Remote to Work Policy, DHCS will, as soon as reasonably possible, supply copies to the County of Orange or its designee as well as DHCS' proposed target date for compliance. For a period of 30 days, DHCS will accept input from the County of Orange or its designee on the proposed changes. DHCS will issue a new policy in a future MEDIL. If the Contractor is unable to comply with these standards, the Contractor will be asked to develop a Plan of Action and Milestones (POA&M) detailing a concrete roadmap to becoming fully compliant with the policy's standard. The POA&M must be provided to the County of Orange for review and approval. Any Contractor who is under a POA&M will be required to provide quarterly updates to the County of Orange until the fully compliant.

VI. AUDIT CONTROLS

A. ***Audit Control Mechanisms.*** The Contractor shall ensure audit control mechanisms are in place that are compliant with the Technical Security Controls within Section V of this Agreement.

B. ***Anomalies.*** When the Contractor or the County of Orange suspects MEDS usage anomalies, the Contractor shall work with the County of Orange to investigate the anomalies and report conclusions of such investigations and remediation to the County of Orange.

C. ***Notification to the County of Orange in event Contractor is subject to other Audit.*** If Contractor is the subject of an audit, compliance review, investigation, or any proceeding that is related to the performance of its obligations pursuant to this Agreement, or is the subject of any judicial or administrative proceeding alleging a violation of law related to the privacy and security of PII, including but not limited to Medi-Cal PII, the Contractor shall promptly notify the County of Orange unless it is legally prohibited from doing so.

VII. PAPER, RECORD, AND MEDIA CONTROLS

A. ***Supervision of Data.*** PII shall not be left unattended at any time, unless it is locked in a file cabinet, file room, desk or office at the individual's place of employment or at home when working remotely. Unattended means that information may be observed by an individual not authorized to access the information.

B. ***Data in Vehicles.*** The Contractor shall have policies that include, based on applicable risk factors, a description of the circumstances under which the Contractor Workers can transport PII, as well as the physical security requirements during transport. A Contractor that chooses to permit its Contractor Workers to leave records unattended in vehicles, shall include provisions in its policies to provide that the PII is stored in a non-visible area such as a trunk, that the vehicle is locked, and that under no circumstances permit PII to be left unattended in a vehicle overnight or for other extended periods of time.

C. ***Public Modes of Transportation.*** PII shall not be left unattended at any time in airplanes, buses, trains, etc., inclusive of baggage areas. This should be included in training due to the nature of the risk.

D. ***Escorting Visitors.*** Visitors to areas where PII is contained shall be escorted, and PII shall be kept out of sight while visitors are in the area.

E. ***Confidential Destruction.*** PII shall be disposed of through confidential means, such as cross cut shredding or pulverizing.

F. ***Removal of Data.*** PII shall not be removed from the premises of Contractor except for justifiable business purposes.

G. ***Faxing.***

1. Faxes containing PII shall not be left unattended and fax machines shall be in secure areas.

2. Faxes shall contain a confidentiality statement notifying persons receiving faxes in error to destroy them and notify the sender.

3. Fax numbers shall be verified with the intended recipient before sending the fax.

H. ***Mailing.***

1. Mailings containing PII shall be sealed and secured from damage or inappropriate viewing of PII to the extent possible.

2. Mailings that include 500 or more individually identifiable records containing PII in a single package shall be sent using a tracked mailing method that includes verification of delivery and receipt.

VIII. NOTIFICATION AND INVESTIGATION OF BREACHES AND SECURITY INCIDENTS

During the term of this Agreement, the Contractor agrees to implement reasonable systems for the discovery and prompt reporting of any breach or security incident, and to take the following steps:

A. ***Initial Notice to the County of Orange:***

The Contractor shall notify the County of Orange using County online incident reporting portal of any suspected security incident, intrusion, or unauthorized access, use, or disclosure of PII or potential loss of PII. When making notification, the following applies:

1. If a suspected security incident involves PII provided or verified by SSA, the Contractor shall immediately notify the County of Orange upon discovery. For more information on SSA data, please see the Definition section of this Agreement.

2. If a suspected security incident does not involve PII provided or verified by SSA, the Contractor shall notify the County of Orange promptly and in no event later than one working day of discovery of:

   a. Unsecured PII if the PII is reasonably believed to have been accessed or acquired by an unauthorized person;
   b. Any suspected security incident which risks unauthorized access to PII and/or;
   c. Any intrusion or unauthorized access, use, or disclosure of PII in violation of this Agreement; or
   d. Potential loss of PII affecting this Agreement.

Notice to County shall include all information known at the time the incident is reported. Contractor shall submit notice via the link County of Orange Incident Reporting Portal and email contact using the information listed in subsection H..

If County online incident reporting portal is unavailable, notice to County can instead be made via email using the County Privacy Incident Report (PIR) form, which the County will coordinate with Contractor.

A breach shall be treated as discovered by the Contractor as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach), who is an employee, officer or other agent of the Contractor.

Upon discovery of a breach, security incident, intrusion, or unauthorized access, use, or disclosure of PII, the Contractor shall take:

1. Prompt corrective action to mitigate any risks or damages involved with the security incident or breach; and
2. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

B. ***Investigation of Security Incident or Breach.*** The Contractor shall immediately investigate such a security incident, breach, or unauthorized use of PII.

C. ***Complete Report.*** Within 10 working days of the discovery the Contractor shall provide any additional information related to the incident requested by the County of Orange. The Contractor shall make reasonable efforts to provide the County of Orange with such information.

The complete report must include an assessment of all known factors relevant to a determination of whether a breach occurred under applicable federal and state laws. The report shall include a full, detailed corrective action plan (CAP) including mitigating measures that were taken to halt and/or contain the improper use or disclosure.

If the County of Orange requests additional information related to the incident, the Contractor shall make reasonable efforts to provide the County of Orange with such information. If necessary, the Contractor shall submit an updated report with revisions and/or additional information after the Completed Report has been provided. The County of Orange will review and determine whether a breach occurred and whether individual notification is required. The County of Orange will maintain the final decision making over a breach determination.

D. ***Notification of Individuals.*** If the cause of a breach is solely attributable to the Contractor or its agents, Contractor shall notify individuals accordingly and shall pay all costs of such notifications as well as any costs associated with the breach. The notifications shall comply with applicable federal and state law. The County of Orange and DHCS shall approve the time, manner, and content of any such notifications and their review and approval must be obtained before the notifications are made. The County of Orange and the Contractor shall work together to ensure that notification of individuals is done in compliance with statutory deadlines within applicable federal and state law.

If the cause of a breach is solely attributable to the County of Orange, the County of Orange shall pay all costs of such notifications as well as any costs associated with the breach. If there is any question as to whether the County of Orange or the Contractor is responsible for the breach or the County of Orange and the Contractor acknowledge that both are responsible for the breach,

the County of Orange and the Contractor shall jointly determine responsibility for purposes of allocating the costs.

1. All notifications (regardless of breach status) regarding beneficiaries' PII shall comply with the requirements set forth in Section 1798.29 of the California Civil Code and Section 17932 of Title 42 of United States Code, inclusive of its implementing regulations, including but not limited to the requirement that the notifications be made without unreasonable delay and in no event later than **60 calendar days** from discovery.

E. ***Responsibility for Reporting of Breaches***

1. ***Breach Attributable to Contractor.*** If the cause of a breach of PII is attributable to the Contractor or its agents, subcontractors, or vendors, the Contractor shall be responsible for all required reporting of the breach.

2. ***Breach Attributable to the County of Orange.*** If the cause of the breach is attributable to the County of Orange, the County of Orange shall be responsible for all required reporting of the breach.

F. ***Coordination of Reporting.*** When applicable law requires the breach be reported to a federal or state agency, or that notice be given to media outlets, the County of Orange and the Contractor shall coordinate to ensure such reporting is compliant with applicable law and prevent duplicate reporting and to jointly determine responsibility for purposes of allocating the costs of such reports, if any.

G. ***Submission of Sample Notification to Attorney General:*** If the cause of the breach is attributable to the Contractor or an agent, subcontractor, or vendor of the Contractor and if notification to more than 500 individuals is required pursuant to California Civil Code section 1798.29, regardless of whether Contractor is considered only a custodian and/or non-owner of the PII, Contractor shall, at its sole expense and at the sole election of the County of Orange, either:

1. Electronically submit a single sample copy of the security breach notification, excluding any personally identifiable information, to the Attorney General pursuant to the format, content, and timeliness provisions of Section 1798.29, subdivision (e). Contractor shall inform the County of Orange Privacy Officer of the time, manner, and content of any such submissions prior to the transmission of such submissions to the Attorney General; or

2. Cooperate with and assist the County of Orange in its submission of a sample copy of the notification to the Attorney General.

H. ***County of Orange Contact Information.*** The Contractor shall utilize the below contact information to direct all communication/notifications of breach and security incidents to the County of Orange. The County of Orange reserves the right to make changes to the contact information by giving written notice to the Contractor. Said changes shall not require an amendment to this Agreement or any other agreement into which it is incorporated.

County of Orange Breach and Security Incident Reporting	
Andrew Alipanah, MBA, CISSP Chief Information Security Officer County of Orange Enterprise Privacy & Cybersecurity 721 S. Parker St., Ste. 200 Orange, CA 92868 Email: Andrew.Alipanah@ocit.oc.gov Telephone: (714) 567-7611	Linda Le, CHC, CHPC, CHP County Privacy Officer County of Orange Enterprise Privacy & Cybersecurity 721 S. Parker St., Suite 200 Orange, CA 92868 Email: privacyofficer@ocgov.com securityadmin@ocit.oc.gov linda.le@ocit.oc.gov Telephone: (714) 834-4082
Karen Vu Procurement Contract Manager, Senior Contracts Services County of Orange Social Services Agency 500 N. State College Blvd. Orange, CA 92868 Email: Karen.vu@ssa.ocgov.com Telephone: 714-541-7785	Alin Buna Procurement Contract Manager, Senior Procurement Services County of Orange Social Services Agency 500 N. State College Blvd. Orange, CA 92868 Email: Alin.buna@ssa.ocgov.com Telephone: 714-541-7767
The preferred method of communication is email, when available. Do not include any PII unless requested by the County of Orange.	

IX. RESERVED

The Contractor shall utilize the below contact information for any PSA-related inquiries or questions. The County of Orange reserves the right to make changes to the contact information by giving written notice to the Contractor. Said changes shall not require an amendment to this Agreement or any other agreement into which it is incorporated. *Please use the contact information listed in Section X of this Agreement for any PII incident or breach reporting.*

PSA Inquiries and Questions
County of Orange Social Services Agency 500 N. State College Blvd. Orange, CA 92868 Email: ssacontractsservices@ssa.ocgov.com

X. COMPLIANCE WITH SSA AGREEMENT

The Contractor agrees to comply with applicable privacy and security requirements in the Computer Matching and Privacy Protection Act Agreement (CMPPA) between SSA and the California Health and Human Services Agency (CalHHS), in the Information Exchange Agreement (IEA) between SSA and DHCS and CDSS, and in the Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with SSA (TSSR), which are incorporated into this Agreement within section V. Technical Security Controls and Exhibit A (available upon request).

If there is any conflict between a privacy and security standard in the CMPPA, IEA or TSSR, and a standard in this Agreement, the most stringent standard shall apply. The most stringent standard means the standard which provides the greatest protection to PII.

If SSA changes the terms of its agreement(s) with DHCS and CDSS, the County of Orange will, as soon as reasonably possible after receipt from DHCS and CDSS, supply copies to the Contractor as well as DHCS' and CDSS' proposed target date for compliance. Once a target date for compliance is determined by SSA, the County of Orange will supply copies of the changed agreement to the Contractor after receipt from DHCS and CDSS, along with the compliance date expected by SSA. If the Contractor is not able to meet the SSA compliance date, the Contractor will be asked to develop a POA&M detailing a concrete roadmap to becoming fully compliant with the policy's standard. The POA&M must be provided to the County of Orange for review and approval. Any Contractor who is under a POA&M will be required to provide quarterly updates to the County of Orange until the fully compliant.

A copy of Exhibit A can be requested by the Contractor from the County of Orange using the contact information listed in Section VIII.H of this Agreement.

XI. COMPLIANCE WITH DEPARTMENT OF HOMELAND SECURITY AGREEMENT

The Contractor agrees to comply with substantive privacy and security requirements in the Computer Matching Agreement (CMA) between the Department of Homeland Security, United States Citizenship and Immigration Services (DHS-USCIS), DHCS and CDSS, which is hereby incorporated into this Agreement (Exhibit B) and available upon request. If there is any conflict between a privacy and security standard in the CMA and a standard in this Agreement, the most stringent standard shall apply. The most stringent standard means the standard which provides the greatest protection to PII.

If DHS-USCIS changes the terms of its agreement(s) with DHCS and CDSS, the County of Orange will, as soon as reasonably possible after receipt from DHCS and CDSS, supply copies to the Contractor as well as DHCS' and CDSS' proposed target date for compliance. Once a target date for compliance is determined by DHS-USCIS, the County of Orange will supply copies of the changed agreement to Contractor after receipt from DHCS and CDSS, along with the compliance date expected by DHS-USCIS. If the Contractor is not able to meet the DHS-USCIS compliance date, the POA&M must be provided to the County of Orange for review and approval. Any Contractor who is under a POA&M will be required to provide quarterly updates to the County of Orange until the fully compliant.

A copy of Exhibit B can be requested by the Contractor from the County of Orange using the contact information listed in Section VIII.H of this Agreement.

XII. CONTRACTOR'S AGENTS, SUBCONTRACTORS, AND VENDORS

The Contractor agrees to enter into written agreements with all agents, subcontractors and vendors that have access to Contractor PII. These agreements will impose, at a minimum, the same restrictions and conditions that apply to the Contractor with respect to PII upon such agents, subcontractors, and vendors. These shall include, (1) restrictions on disclosure of PII, (2) conditions regarding the use of appropriate administrative, physical, and technical safeguards to protect PII, and, where relevant, (3) the requirement that any breach, security incident, intrusion, or unauthorized access, use, or disclosure of PII be reported to the Contractor. If the agents, subcontractors, and vendors of Contractor access data provided to the County of Orange by DHCS and/or CDSS by SSA or DHS-USCIS, the Contractor shall also incorporate the Agreement's Exhibits into each subcontract or subaward with agents, subcontractors, and vendors.

Contractors who would like assistance or guidance with this requirement are encouraged to coordinate with the County of Orange.

XIII. ASSESSMENTS AND REVIEWS

In order to enforce this Agreement and ensure compliance with its provisions and Exhibits, the Contractor agrees to assist the County of Orange in performing compliance assessments. These assessments may involve compliance review questionnaires, and/or review of the facilities, systems, books, and records of the Contractor, with reasonable notice from the County Orange. Such reviews shall be scheduled at times that take into account the operational and staffing demands. The Contractor agrees to promptly remedy all violations of any provision of this Agreement and certify the same to the County of Orange in writing, or to enter into a POA&M with the County of Orange containing deadlines for achieving compliance with specific provisions of this Agreement.

XIV. ASSISTANCE IN LITIGATION OR ADMINISTRATIVE PROCEEDINGS

In the event of litigation or administrative proceedings involving the County of Orange based upon claimed violations by the Contractor of the privacy or security of PII or of federal or state laws or agreements concerning privacy or security of PII, the Contractor shall make all reasonable effort to make itself and Contractor Workers assisting in the administration of Medi-Cal programs and using or disclosing PII available to the County of Orange at no cost to the County of Orange to testify as witnesses. The County of Orange shall also make all reasonable efforts to make itself and any subcontractors, agents, and employees available to the Contractor at no cost to the Contractor to testify as witnesses, in the event of litigation or administrative proceedings involving the Contractor based upon claimed violations by the County of Orange of the privacy or security of PII or of state or federal laws or agreements concerning privacy or security of PII.

XV. AMENDMENT OF AGREEMENT

The County of Orange and the Contractor acknowledge that federal and state laws relating to data security and privacy are rapidly evolving and that amendment of this Agreement may be required to ensure compliance with such changes. Upon request by the County of Orange, the Contractor agrees to promptly enter into negotiations with the County of Orange concerning an amendment to this Agreement as may be needed by changes in federal and state laws and regulations or NIST 800-53. In addition to any other

lawful remedy, the County of Orange may terminate this Agreement upon 30 days written notice if the Contractor does not promptly agree to enter into negotiations to amend this Agreement when requested to do so or does not enter into an amendment that the County of Orange deems necessary.

XVI. TERMINATION

This Agreement shall terminate on September 1, 2028, regardless of the date the Agreement is executed by the parties. The parties can agree in writing to extend the term of the Agreement. Contractor's requests for an extension shall be approved by the County of Orange and limited to no more than a six (6) month extension.

A. ***Survival:*** All provisions of this Agreement that provide restrictions on disclosures of PII and that provide administrative, technical, and physical safeguards for the PII in the Contractor's possession shall continue in effect beyond the termination or expiration of this Agreement and shall continue until the PII is destroyed or returned to the County of Orange.

XVII. TERMINATION FOR CAUSE

Upon the County of Orange's knowledge of a material breach or violation of this Agreement by the Contractor, the County of Orange may provide an opportunity for the Contractor to cure the breach or end the violation and may terminate this Agreement if the Contractor does not cure the breach or end the violation within the time specified by the County of Orange. This Agreement may be terminated immediately by the County of Orange if the Contractor has breached a material term and the County of Orange determines, in its sole discretion, that cure is not possible or available under the circumstances. Upon termination of this Agreement, the Contractor shall return or destroy all PII in accordance with Section VII, above. The provisions of this Agreement governing the privacy and security of the PII shall remain in effect until all PII is returned or destroyed and the County of Orange receives a certificate of destruction.

ATTACHMENT C - INFORMATION TECHNOLOGY SECURITY GUIDELINES

All contractors who contract with the County of Orange ("County") shall work cooperatively to assist County in achieving the objectives and abide by the applicable terms under these Guidelines for all Controls one (1) thru six (6) below at all times during the term of its contract with County.

1. ASSET MANAGEMENT

Asset management establishes an organization's inventory of fixed and controlled assets and defines how these assets are managed during their lifecycle to ensure sustained productivity in support of the organization's critical services. An event that disrupts an asset can inhibit the organization from achieving its mission. An asset management program helps identify appropriate strategies that shall allow the assets to maintain productivity during disruptive events. There are four broad categories of assets: people, information, technology, and facilities.

The Cybersecurity Program strives to achieve and maintain appropriate protection of IT assets. Loss of accountability of IT assets could result in a compromise or breach of IT systems and/or a compromise or breach of sensitive or privacy data.

A. GOALS AND OBJECTIVES

1. Services are identified and prioritized.
2. Assets are inventoried, and the authority and responsibility for these assets is established.
3. The relationship between assets and the services they support is established.
4. The asset inventory is managed.
5. Access to assets is managed.
6. Information assets are categorized and managed to ensure the sustainment and protection of the critical service.
7. Facility assets supporting the critical service are prioritized and managed.

B. ASSET MANAGEMENT POLICY STATEMENTS

1. **Services Inventory**
   a. Departments and/or contractors shall maintain an inventory of its services. This listing shall be used by the department to assist with its risk management analysis.
2. **Asset Inventory – Information**
   a. All information that is created or used within the County's trusted environment in support of County business activities shall be considered the property of the County. All County property shall be used in compliance with this policy.
   b. County information is a valuable asset and shall be protected from unauthorized disclosure, modification, or destruction. Prudent information security standards and

practices shall be implemented to ensure that the integrity, confidentiality, and availability of County information are not compromised. All County information shall be protected from the time of its creation through its useful life and authorized disposal.

c. Departments and/or contractors shall establish internal procedures for the secure handling and storage of all electronically maintained County information that is owned or controlled by the department.

3. **Asset Inventory - Technology (Devices, Software)**

a. Departments shall maintain an inventory of all department managed devices that connect to County network resources or processes, stores, or transmits County data including but not limited to:

i. Desktop computers,

ii. Laptop Computers,

iii. Tablets (iPads and Android devices),

iv. Mobile Phones (basic cell phones),

v. Smart Phones (iPhones, Blackberry, Windows Phones and Android Phones),

vi. Servers,

vii. Storage devices,

viii. Network switches,

ix. Routers,

x. Firewalls,

xi. Security Appliances,

xii. Internet of Things (IoT) devices,

xiii. Printers,

xiv. Scanners,

xv. Kiosks and Thin clients,

xvi. Mainframe Hardware, and

xvii. VoIP Phones.

b. Asset inventory shall map assets to the services they support.

c. Departments and/or contractors shall adopt a standard naming convention for devices (naming convention to be utilized as devices are serviced or purchased).

d. Each department and/or contractor shall ensure that all software used on County systems and in the execution of County business shall be used legally and in compliance with licensing agreements.

4. **Asset Inventory - Facilities**

   a. Departments and/or contractors shall maintain an inventory of its facilities. This listing shall be used by the department to assist with its risk management analysis.

   b. Departments and/or contractors shall identify the facilities used by its critical services.

5. **Access Controls**

   a. Departments and/or contractors shall establish a procedure that ensures only users with legitimate business needs to access County IT resources are provided with user accounts.

   b. Access to County information systems and information systems data shall be based on each user's access privileges. Access controls shall ensure that even legitimate users cannot access stored information unless they are authorized to do so. Access control should start by denying access to everything, and then explicitly granting access according to the "need to know" principle.

   c. Access to County information and County information assets should be based on the principle of "least privilege," that is, grant no user greater access privileges to the information or assets than County responsibilities demand.

   d. The owner of each County system, or their designee, provides written authorization for all internal and external user access.

   e. lAll access to internal County computer systems shall be controlled by an authentication method involving a minimum of a user identifier (ID) and password combination that provides verification of the user's identity.

   f. All County workforce members are to be assigned a unique user ID to access the network, as applicable.

   g. A user account shall be explicitly assigned to a single, named individual. No group or shared computer accounts are permissible except when necessary and warranted due to legitimate business needs. Such need shall be documented prior to account creation and accounts activated only when necessary.

   h. User accounts shall not be shared with others including, but not limited to, someone whose access has been denied or terminated.

   i. Departments and/or contractors shall conduct regular reviews of the registered users' access level privileges. System owners shall provide user listings to departments for confirmation of user's access privileges.

6. **Asset Sanitation/Disposal**

   a. Unless approved by County management, no County computer equipment shall be removed from the premises.

   b. Prior to re-deployment, storage media shall be appropriately cleansed to prevent unauthorized exposure of data.

c. Surplus, donation, disposal or destruction of equipment containing storage media shall be appropriately disposed according to the terms of the equipment disposal services contract.

d. Sanitization methods for media containing County information shall be in accordance with NSA (National Security Agency) standards (for example, clearing, purging, or destroying).

e. Disposal of equipment shall be done in accordance with all applicable County, state or federal surplus property and environmental disposal laws, regulations or policies.

2. CONTROLS MANAGEMENT

The Controls Management domain focuses on the processes by which an organization plans, defines, analyzes, and assesses the controls that are implemented internally. This process helps the organization ensure the controls management objectives are satisfied.

This domain focuses on the resilience controls that allow an organization to operate during a time of stress. These resilience controls are implemented in the organization at all levels and require various levels of management and staff to plan, define, analyze, and assess.

A. GOALS AND OBJECTIVES

1. Control objectives are established.
2. Controls are implemented.
3. Control designs are analyzed to ensure they satisfy control objectives.
4. Internal control system is assessed to ensure control objectives are met.

B. CONTROL MANAGEMENT POLICY STATEMENTS

1. Physical and Environmental Security

a. Procedures and facility hardening measures shall be adopted to prevent attempts at and detection of unauthorized access or damage to facilities that contain County information systems and/or processing facilities.

b. Restricted areas within facilities that house sensitive or critical County information systems shall, at a minimum, utilize physical access controls designed to permit access by authorized personnel only.

c. Physical protection measures against damage from external and environmental threats shall be implemented by all departments as appropriate.

d. Access to any office, computer room, or work area that contains sensitive information shall be physically restricted from unauthorized access.

e. Access points such as delivery and loading areas and other points where unauthorized persons may enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access. An example of this would be separating the two areas by a badge-only accessible door.

f. Continuity of power shall be provided to maintain the availability of critical equipment and information systems.

g. Power and telecommunications cabling carrying data or supporting information services shall be protected from interception or damage. Different, yet appropriate methods shall be utilized for internal and external cabling.

h. Equipment shall be properly maintained to ensure its continued availability and integrity.

i. All shared IT infrastructure by more than one department shall meet countywide security policy for facility standards, availability, access, data & network security.

2. **Network Segmentation**
NOTE: This section is applicable to Departments that manage their own network devices.

a. Segment (e.g., VLANs) the network into multiple, separate zones (based on trust levels of the information stored/transmitted) to provide more granular control of system access and additional intranet boundary defenses. Whenever information flows over a network of lower trust level, the information shall be encrypted.

b. Segment the network into multiple, separate zones based on the devices (servers, workstations, mobile devices, printers, etc.) connected to the network.

c. Create separate network segments (e.g., VLANs) for BYOD (bring your own device) systems or other untrusted devices.

d. The network infrastructure shall be managed across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

3. **Mobile Computing Devices**
To ensure that Mobile Computing Devices (MCDs) do not introduce threats into systems that process or store County information, departments' and/or contractors' management shall:

a. Establish and manage a process for authorizing, issuing and tracking the use of MCDs.

b. Permit only authorized MCDs to connect to County information assets or networks that store, process, transmit, or connects to County information and information assets.

c. Implement applicable access control requirements in accordance with this guideline, such as the enforcement of a system or device lockout after 15 minutes of inactivity requiring re-entering of a password to unlock.

d. Install an encryption algorithm that meets or exceeds industry recommended encryption standard for any MCD that will be used to store County information.

e. Ensure that MCDs are configured to restrict the user from circumventing the authentication process.

f. Provide security awareness training to County employees that informs MCD users regarding MCD restrictions.

g. Label MCDs with County address and/or phone number so that the device can be returned to the County if recovered.

h. The installation of any software, executable, or other file to any County computing device is prohibited if that software, executable, or other file downloaded by, is owned by, or was purchased by an employee or contractor with his or her own funds unless approved by the department.

4. **Personally Owned Devices**
Personal computing devices include, but are not limited to, removable media such as thumb or USB drives, external hard drives, laptop or desktop computers, cellular phones, or personal digital assistants (PDA's) owned by or purchased by employees, contract personnel, or other non-County users.

a. The connection of any computing device not owned by the County to a County network (except the Public Wi-Fi provided for public use) or computing device is prohibited unless previously approved.

b. The County authorizes the use of personal devices to access resources that do not traverse the County network directly. Such resources include County's SaaS applications. Access to some agency specific applications, e.g. applications that are subject to compliance regulations may require prior approval of the County CISO and the associated Department Head.

c. The County will respect the privacy of a user's voluntary use of a personally owned device to access County IT resources.

d. The County will only request access to the personally owned device in order to implement security controls; to respond to litigation hold (aka: e-discovery) requests arising out of administrative, civil, or criminal directives, Public Record Act requests, and subpoenas; or as otherwise required or permitted by applicable state or federal laws. Such access will be performed by an authorized technician or designee using a legitimate software process.

5. **Logon Banners and Warning Notices**

a. At the time of network login, the user shall be presented with a login banner.

b. All computer systems that contain or access County information shall display warning banners informing potential users of conditions of use consistent with state and federal laws.

c. Warning banners shall remain on the screen until the user takes explicit actions to log on to the information system.

d. The banner message shall be placed at the user authentication point for every computer system that contains or accesses County information. The banner message may be placed on an initial logon screen in situations where the logon provides access to multiple computer systems.

e. At a minimum, banner messages shall provide appropriate privacy and security information and shall contain information informing potential users that:

   i. User is accessing a government information system for conditions of use consistent with state and federal information security and privacy protection laws.

   ii. System usage may be monitored, recorded, and subject to audit.

   iii. Unauthorized use of the system is prohibited and subject to criminal and civil penalties.

   iv. Use of the system indicates consent to monitoring and recording.

6. **Authentication**

   a. Authenticate user identities at initial connection to County resources.

   b. Authentication mechanisms shall be appropriate to the sensitivity of the information contained.

   c. Users shall not receive detailed feedback from the authenticating system on failed logon attempts.

7. **Passwords**

   a. County approved password standards and/or guidelines shall be applied to access County systems. These standards extend to mobile devices and personally owned devices used for work.

   b. 2.Passwords are a primary means to control access to systems and shall therefore be selected, used, and managed to protect against unauthorized discovery or usage. Passwords shall satisfy the following complexity rule:

      i. Passwords will contain a minimum of one (1) upper case letter

      ii. Passwords will contain a minimum of one (1) lower case letter

      iii. Passwords will contain a minimum of one (1) number: 1- 0

      iv. Passwords will contain a minimum of one (1) special character: !,@,#,$,%,^,&,*,(,)

      v. Password characters will not be sequential (Do not use: ABCD , This is ok: ACDB)

      vi. Passwords characters will not be repeated in a row (Do not use: P@$$S. This is ok: P@S)

      vii. COMPLEX PASSWORD EXAMPLE: P@$SWoRd13

viii. Passphrases example: The$kyIsBlue2day

ix. Passwords cannot contain the user's full name or network login.

c. Passwords shall have a minimum length of twelve (12) characters.

d. Passwords shall not be reused for twelve (12) iterations.

e. Departments and/or contractors shall require users to change their passwords periodically (e.g., every 90 days at the maximum). Changing passwords more often than 90 days is encouraged.

f. Network and application systems shall be configured to enforce automatic expiration of passwords at regular intervals (e.g., every 90 days at the maximum) when the technology is feasible or available.

g. Newly created accounts shall be assigned a randomly generated password prior to account information being provided to the user.

h. No user shall give his or her password to another person under any circumstances. Workforce members who suspect that their password has become known by another person shall change their password immediately and report their suspicion to management.

i. Users who have lost or forgotten their passwords shall make any password reset requests themselves without using a proxy (e.g., another County employee) unless approved by management. Prior to processing password change requests, the requester shall be authenticated to the user account in question. (e.g., Verification with user's supervisor or the use of passphrases can be used for this authentication process.) New passwords shall be provided directly and only to the user in question.

j. When technologically feasible, a new or reset password shall be set to expire on its initial use at log on so that the user is required to change the provided password to one known only to them.

k. All passwords are to be treated as sensitive information.

l. User Accounts shall be locked after five consecutive invalid logon attempts within a 24-hour period. The lockout duration shall be at least 30 minutes or until a system administrator enables the user ID after investigation. These features shall be configured as indicated when the technology is feasible or available.

m. All systems containing sensitive information shall not allow users to have multiple concurrent sessions on the same system when the technology is feasible or available.

C. **Inactivity Timeout and Restricted Connection Times**

1. Automatic lockouts for system devices, including workstations and mobile computing devices, after no more than 15 minutes of inactivity.

2. Automated screen lockouts shall be used wherever possible using a set time increment (e.g., 15 minutes of non-activity). In situations where it is not possible to automate a lockout, operational procedures shall be implemented to instruct users to lock the terminal or equipment so that unauthorized individuals cannot make use of the system. Once logged on, workforce members shall not leave their computer unattended or available for someone else to use.
3. When deemed necessary, user logins and data communications may be restricted by time and date configurations that limit when connections shall be accepted.

D. **Account Monitoring**

1. Access to a County network and its resources shall be strictly controlled, managed, and reviewed to ensure only authorized users gain access based on the privileges granted. (e.g., Kiosks provide physical and public access to County networks. These shall be secured to ensure County resources are not accessed by unauthorized users.)
2. The control mechanisms for all types of access to County IT resources by contractors, customers or vendors are to be documented.
3. Monitor account usage to determine dormant accounts that have not been used for a given period, such as 45 days, notifying the user or user's manager of the dormancy.
4. After a longer period, such as 60 days, the account shall be disabled by the system when the technology is feasible or available.
5. On a periodic basis, such as quarterly or at least annually, departments shall require that managers match active employees and contractors with each account belonging to their managed staff. Security or system administrators shall then determine whether to disable accounts that are not assigned to active employees or contractors.

E. **Administrative Privileges**

1. Systems Administrators shall use separate administrative accounts, which are different from their end user account (required to have an individual end user account), to conduct system administration tasks.
2. Administrative accounts shall only be granted to individuals who have a job requirement to conduct systems administration tasks.
3. Administrative accounts shall be requested in writing and must be approved by the Department Head or designated representative using the Security Review and Approval Process.
4. Systems Administrator accounts that access County enterprise-wide systems or have enterprise-wide impact shall be approved by the CISO using the Security Review and Approval Process.
5. Systems Administrators shall use separate administrative accounts to manage Mobile Device Management (MDM) platforms but may use the local user's credentials when configuring a mobile phone or tablet device.

6. All passwords for privileged system-level accounts (e.g., root, enable, OS admin, application administration accounts, etc.) shall comply with Controls Management B.7.

F. **Remote Access**

1. Departments and/or contractors shall take appropriate steps, including the implementation of appropriate encryption, user authentication, and virus protection measures, to mitigate security risks associated with allowing users to use remote access or mobile computing methods to access County information systems.
2. Remote access privileges shall be granted to County workforce members only for legitimate business needs and with the specific approval of department management.
3. All remote access implementations that utilize the County's trusted network environment and that have not been previously deployed within the County shall be submitted to and reviewed by the County. A memorandum of understanding (MOU) shall be utilized for this submittal and review process. This is required for any Suppliers utilizing remote access to conduct maintenance.
4. Remote sessions shall be terminated after 15 minutes of inactivity requiring the user to authenticate again to access County resources.
5. All remote access infrastructures shall include the capability to monitor and record a detailed audit trail of each remote access attempt.
6. All users of County networks and computer systems are prohibited from connecting and/or activating unauthorized dial-up or broadband modems on workstations, laptops, or other computing devices that are simultaneously connected to any County network.
7. Periodic assessments shall be performed to identify unauthorized remote connections. Results shall be used to address any vulnerabilities and prioritized according to criticality.
8. Users granted remote access to County IT infrastructure shall follow all additional policies, guidelines and standards related to authentication and authorization as if they were connected locally. For example, this applies when mapping to shared network drives.
9. Users attempting to use external remote access shall utilize a County-approved multi-factor authentication process.
10. All remote access implementations that involve non-County infrastructures shall be reviewed and approved by both the department and the County. This approval shall be received prior to the start of such implementation.
11. Remote access privileges to County IT resources shall not be given to contractors and customers unless department management determines that these individuals or organizations have a legitimate business need for such access. If such access is granted, it shall be limited to those privileges and conditions required for the performance of the specified work.

G. **Wireless Access**

1. Departments and/or contractors shall take appropriate steps, including the implementation of appropriate encryption, user authentication, device authentication and malware protection measures, to mitigate risks to the security of County data and information systems associated with the use of wireless network access technologies.
2. Only wireless systems that have been evaluated for security by both department management and the County shall be approved for connectivity to County networks.
3. County data that is transmitted over any wireless network shall be protected in accordance with the sensitivity of the information.
4. All access to County networks or resources via unapproved wireless communication technologies is prohibited. This includes wireless systems that may be brought into County facilities by visitors or guests. Employees, contractors, vendors and customers are prohibited from connecting and/or activating wireless connections on any computing device that are simultaneously connected to any County network, either locally or remotely.
5. Each department and/or contractor shall make a regular, routine effort to ensure that unauthorized wireless networks, access points, and/or modems are not installed or configured within its IT environments. Any unauthorized connections described above shall be disabled immediately.

H. **System and Network Operations Management**

1. Operating procedures and responsibilities for all County information processing facilities shall be formally authorized, documented, and updated.
2. Departments and/or contractors shall establish controls to ensure the security of the information systems networks that they operate.
3. Operational system documentation for County information systems shall be protected from unauthorized access.
4. System utilities shall be available to only those users who have a business case for accessing the specific utility.

I. **System Monitoring and Logging**

1. Systems operational staff shall maintain appropriate log(s) of activities, exceptions and information security events involving County information systems and services.
2. Each department and/or contractor shall maintain a log of all faults involving County information systems and services.
3. Logs shall be protected from unauthorized access or modifications wherever they reside.
4. The clocks of all relevant information processing systems and attributable logs shall be synchronized with an agreed upon accurate time source such as an established Network Time Protocol (NTP) service.

5. Auditing and logging of user activity shall be implemented on all critical County systems that support user access capabilities.
6. Periodic log reviews of user access and privileges shall be performed in order to monitor access of sensitive information.

J. **Malware Defenses**

1. Departments shall implement endpoint security on computing devices connected to the County network. Endpoint security may include one or more of the following software: anti-virus, anti-spyware, personal firewall, host-based intrusion detection (IDS), network-based intrusion detection (IDS), intrusion prevention systems (IPS), and whitelisting and blacklisting of applications, web sites, and IP addresses.
2. Special features designed to filter out malicious software contained in either email messages or email attachments shall be implemented on all County email systems.
3. Where feasible, any computing device, including laptops and desktop PCs, that has been connected to a non-County infrastructure (including employee home networks) and subsequently used to connect to the County network shall be verified that it is free from viruses and other forms of malicious software prior to attaining connectivity to the County network.

K. **Data Loss Prevention**

1. Departments and/or contractor shall implement host-based Data Loss Prevention (DLP) to reduce the risk of data breach related to sensitive information.
2. Departments and/or contractors shall deploy encryption software on mobile devices containing sensitive.

L. **Data Transfer**

1. Agreements shall be implemented for the exchange of information between the County and other entities. As well as between departments.
2. County information accessed via electronic commerce shall have security controls implemented based on the assessed risk.

M. **Encryption**

1. The decision to use cryptographic controls and/or data encryption in an application shall be based on the level of risk of unauthorized access and the sensitivity of the data that is to be protected.
2. The decision to use cryptographic controls and/or data encryption on a hard drive shall be based on the level of risk of unauthorized access and the sensitivity of the data that is to be protected.
3. Where appropriate, encryption shall be used to protect confidential application data that is transmitted over open, untrusted networks, such as the Internet.
4. When cryptographic controls are used, procedures addressing the following areas shall be established by each department:

a. Determination of the level of cryptographic controls

b. Key management/distribution steps and responsibilities

5. Encryption keys shall be exchanged only using secure methods of communication.

N. **System Acquisition and Development**

1. Departments and/or contractors shall identify all business applications that are used by their users in support of primary business functions. This includes all applications owned and/or managed by the department as well as other business applications that are used by the department but owned and/or managed by other County organizations. All business applications used by a department shall be documented in the department's IT security plan as well as their Business Impact Analysis (BIA) for critical rating (RTO) and continuity purposes.

2. An application owner shall be designated for each internal department business application.

3. All access controls associated with business applications shall be commensurate with the highest level of data used within the application. These same access controls shall also adhere to the policy provided in Section 1.2.5: Access Controls.

4. Security requirements shall be incorporated into the evaluation process for all commercial software products that are intended to be used as the basis for a business application. The security requirements in question shall be based on requirements and standards specified in this guideline.

5. In situations where data needs to be isolated because there would be a conflict of interest, data security shall be designed and implemented to ensure that isolation.

O. **Business Requirements**

1. The business requirements definition phase of system development shall contain a review to ensure that the system shall adhere to County information security standards.

P. **System Files**

1. Operating system files, application software and data shall be secured from unauthorized use or access.

2. Clear-text data that results from testing shall be handled, stored, and disposed of in the same manner and using the same procedures as are used for production data.

3. System tests shall be performed on data that is constructed specifically for that purpose.

4. System testing shall not be performed on operational data unless the necessary safeguards are in place.

5. A combination of technical, procedural and physical safeguards shall be used to protect application source code from unintentional or unauthorized modification or destruction. All County proprietary information, including source code, needs to be protected through appropriate role-based access controls. An example of this is a

change control tool that records all changes to source code including new development, updates, and deletions, along with check-in and check-out information.

Q. **System Development & Maintenance**

1. The development of software for use on County information systems shall have documented change control procedures in place to ensure proper versioning and implementation.
2. When preparing to upgrade any County information systems, including an operating system, on a production computing resource; the process of testing and approving the upgrade shall be completed in advance in order to minimize potential security risks and disruptions to the production environment.
3. Any outside suppliers used for maintenance that are visitors to the facility are to be escorted and monitored while performing maintenance to critical systems. This does not apply to contractors that are assigned to work at the facility.
4. Systems shall be hardened, and logs monitored to ensure the avoidance of the introduction and exploitation of malicious code.
5. All County workforce members, including contractors, shall not create, execute, forward, or introduce computer code designed to self-replicate, damage, or impede the performance of a computer's memory, storage, operating system, or application software.
6. In conjunction with other access control policies, any opportunity for information leakage shall be prevented through good system design practices.
7. Departments and/or contractors are responsible for managing outsourced software development related to department-owned IT systems.

R. **System Requirements**

1. Any system that processes or stores County Information shall:
   a. Baseline configuration shall incorporate Principle of Least Privilege and Functionality.
   b. Systems shall be deployed where feasible to utilize existing County authentication methods.
   c. Session inactivity timeouts shall be implemented for all access into and from County networks.
   d. All applications are to have access controls unless specifically designated as a public access resource.
   e. Meet the password requirements defined in Section 2.2.7: Passwords.
   f. Strictly control access enabling only privileged users or supervisors to override system controls or the capability of bypassing data validation or editing problems.
   g. Monitor special privilege access, e.g. administration accounts.

h. Restrict authority to change master files to persons independent of the data processing function.

i. Have access control mechanisms to prevent unauthorized access or changes to data, especially, the server file systems that are connected to the Internet, even behind a firewall.

j. Be capable of routinely monitoring the access to automated systems containing County Information.

k. Log all modifications to the system files.

l. Limit access to system utility programs to necessary individuals with specific designation.

m. Delete or disable all default accounts.

n. Restrict access to server file-system controls to ensure that all changes such as direct write, write access to system areas and software or service changes shall be applied only through the appropriate change control process.

o. Restrict access to server-file-system controls that allow access to other users' files.

p. Ensure that servers containing user credentials shall be physically protected, hardened and monitored to prevent inappropriate use.

S. **Procurement Controls**

1. Breach notification requirements clause to be included in new or renewal contracts for systems containing sensitive information.

2. Contractor shall report to the County within 24 hours as defined in this contract when Contractor becomes aware of any suspected data breach of contractor's or subcontractor's systems involving County's data.

3. Departments shall review all procurements and renewals for software and equipment (hosted/managed by the vendor) that transmits, stores, or processes sensitive information to ensure that contractors are aware of and are in compliance with County's cybersecurity policies, if applicable. Departments shall obtain documentation supporting the business partners, contractors, or consultants' compliance with County's cybersecurity policies such as:

   a. SOC 1 Type 2

   b. SOC 2 Type 2

   c. Security Certifications (ISO, PCI, etc.)

   d. FedRAMP certification

   e. Penetration Test Results

T. **IT Services Provided to Public**

1. Public access to County electronic information resources shall provide desired services in accordance with safeguards designed to protect County resources. All County electronic information resources are to be reviewed at least quarterly.

U. **Removable Media**

1. When no longer required, the contents of removable media shall be permanently destroyed or rendered unrecoverable in accordance with applicable department, County, state, or federal record disposal and/or retention requirement.

3. CONFIGURATION & CHANGE MANAGEMENT

Configuration and Change Management ("CCM") is the process of maintaining the integrity of hardware, software, firmware, and documentation related to the configuration and change management process. CCM is a continuous process of controlling and approving changes to information or technology assets or related infrastructure that support the critical services of an organization. This process includes the addition of new assets, changes to assets, and the elimination of assets.

Cybersecurity is an integral component to information systems from the onset of the project or acquisition through implementation of:

A. Application and system security

B. Configuration management

C. Change control procedures

D. Encryption and key management

E. Software maintenance, including but not limited to, upgrades, antivirus, patching and malware detection response systems

As the complexity of information systems increases, the complexity of the processes used to create these systems also increases, as does the probability of accidental errors in configuration. The impact of these errors puts data and systems that may be critical to business operations at significant risk of failure that could cause the organization to lose business, suffer damage to its reputation, or close completely. Having a CCM process to protect against these risks is vital to the overall security posture of the organization.

A. GOALS AND OBJECTIVES

1. The lifecycle of assets is managed.
2. The integrity of technology and information assets is managed.
3. Asset configuration baselines are established.

B. CONFIGURATION & CHANGE MANAGEMENT POLICY STATEMENTS

1. Changes to all information processing facilities, systems, software, or procedures shall be strictly controlled according to formal change management procedures.

2. Changes impacting security appliances managed by OCIT (e.g., security architecture, security appliances, County firewall, Website listings, application listings, email gateway, administrative accounts) shall be reviewed by County in accordance with the County Security Review and Approval Process.
3. Only authorized users shall make any changes to system and/or software configuration files.
4. Only authorized users shall download and/or install operating system software, service-related software (such as web server software), or other software applications on County computer systems without prior written authorization from department IT management. This includes, but is not limited to, free software, computer games and peer-to-peer file sharing software.
5. Each department and/or contractor shall develop a formal change control procedure that outlines the process to be used for identifying, classifying, approving, implementing, testing, and documenting changes to its IT resources.
6. Each department and/or contractor shall conduct periodic audits designed to determine if unauthorized software has been installed on any of its computers.
7. As appropriate, segregation of duties shall be implemented by all County departments to ensure that no single person has control of multiple critical systems and the potential for misusing that control.
8. Production computing environments shall be separated from development and test computing environments to reduce the risk of one environment adversely affecting another.
9. System capacity requirements shall be monitored, and usage projected to ensure the continual availability of adequate processing power, bandwidth, and storage.
10. System acceptance criteria for all new information systems and system upgrades shall be defined, documented, and utilized to minimize risk of system failure.

4. VULNERABILITY MANAGEMENT

The Vulnerability Management domain focuses on the process by which organizations identify, analyze, and manage vulnerabilities in a critical service's operating environment.

A. GOALS AND OBJECTIVES

1. Preparation for vulnerability analysis and resolution activities is conducted.
2. A process for identifying and analyzing vulnerabilities is established and maintained.
3. Exposure to identified vulnerabilities is managed.
4. The root causes of vulnerabilities are addressed.

B. VULNERABILITY MANAGEMENT POLICY STATEMENTS

1. Departments and/or contractors shall develop and maintain a vulnerability management process as part of its Cybersecurity Program.

5. CYBERSECURITY INCIDENT MANAGEMENT

Information Security Incident Management establishes the policy to be used by each department and/or contractor in planning for, reporting on, and responding to computer security incidents. For these purposes an incident is defined as any irregular or adverse event that occurs on a County system or network. The goal of incident management is to mitigate the impact of a disruptive event. To accomplish this goal, an organization establishes processes that:

- detect and identify events
- triage and analyze events to determine whether an incident is underway
- respond and recover from an incident
- improve the organization's capabilities for responding to a future incident

This domain defines management controls for addressing cyber incidents. The controls provide a consistent and effective approach to Cyber Incident Response aligned with Orange County's Cyber Incident Response Plan, to include:

- Collection of evidence related to the cyber incident as appropriate
- Reporting procedures including any and all statutory reporting requirements
- Incident remediation
- Minimum logging procedures
- Annual testing of the plan

A. GOALS AND OBJECTIVES

1. A process for identifying, analyzing, responding to, and learning from incidents is established.
2. A process for detecting, reporting, triaging, and analyzing events is established.
3. Incidents are declared and analyzed.
4. A process for responding to and recovering from incidents is established.
5. Post-incident lessons learned are translated into improvement strategies.

B. CYBERSECURITY INCIDENT MANAGEMENT POLICY STATEMENTS

1. Cybersecurity incident management procedures shall be established within each department and/or contractor to ensure quick, orderly, and effective responses to security incidents. In the event a department has not established these procedures, the department may adopt the County's Cyber Incident Response Plan. The steps involved in managing a security incident are typically categorized into six stages:
   a. System preparation
   b. Problem identification

c. Problem containment

d. Problem eradication

e. Incident recovery

f. Lessons learned

2. The department shall act as the liaison between applicable parties during a cybersecurity incident. The department shall be the primary point of contact for all IT security issues.

3. A designated security contact for all cybersecurity incidents.

4. Departments and/or contractors shall conduct periodic (at least annually) cybersecurity incident scenario sessions for personnel associated with the cybersecurity incident handling team to ensure that they understand current threats and risks, as well as their responsibilities in supporting the cybersecurity incident handling team.

5. Departments and/or contractors shall develop and document procedures for reporting cybersecurity incidents. For example, all employees, contractors, and customers of County information systems shall be required to note and report any observed or suspected security weaknesses in systems to management. In the event a department has not established these procedures, the department may adopt the County's Cyber Incident Response Plan.

6. Each department and/or contractor shall familiarize its employees on the use of its cybersecurity incident reporting procedures.

7. Contact with local authorities, including law enforcement, shall be conducted through an organized, repeatable process that is both well documented and communicated.

8. Contact with special interest groups, including media and labor relations, shall be conducted through an organized, repeatable process that is both well documented and communicated.

9. Where a follow-up action against an entity after a cybersecurity incident shall involve civil or criminal legal action, evidence shall be collected, retained, and presented to conform to the rules for evidence as demanded by the relevant jurisdiction(s). At the Department's discretion, they may obtain the services of qualified external professionals to complete these tasks.

10. Departments shall report cybersecurity incidents to the County pursuant to the Contract.

6. SERVICE CONTINUITY MANAGEMENT

Service continuity planning is one of the more important aspects of resilience management because it provides a process for preparing for and responding to disruptive events, whether natural or man-made. Operational disruptions may occur regularly and can scale from so small that the impact is essentially negligible to so large that they could prevent an organization from achieving its mission. Services that are most important to an organization's ability to meet its mission are

considered essential and are focused on first when responding to disruptions. The process of identifying and prioritizing services and the assets that support them is foundational to service continuity.

Service continuity planning provides the organization with predefined procedures for sustaining essential operations in varying adverse conditions, from minor interruptions to large-scale incidents. For example, a power interruption or failure of an IT component may necessitate manual workaround procedures during repairs. A data center outage or loss of a business or facility housing essential services may require the organization to recover business or IT operations at an alternate location.

The process of assessing, prioritizing, planning and responding to, and improving plans to address disruptive events is known as service continuity. The goal of service continuity is to mitigate the impact of disruptive events by utilizing tested or exercised plans that facilitate predictable and consistent continuity of essential services.

This domain defines requirements to document, implement and annually test plans, including the testing of all appropriate cybersecurity provisions, to minimize impact to systems or processes from the effects of major failures of information systems or disasters via adoption and annual testing of:

- Business Continuity Plan
- Disaster Recovery Plan
- Cyber Incident Response Plan

Business Continuity is intended to counteract interruptions in business activities and to protect critical business processes from the effects of significant disruptions. Disaster Recovery provides for the restoration of critical County assets, including IT infrastructure and systems, staff, and facilities.

A. GOALS AND OBJECTIVES

1. Service continuity plans for high-value services are developed.
2. Service continuity plans are reviewed to resolve conflicts between plans.
3. Service continuity plans are tested to ensure they meet their stated objectives.
4. Service continuity plans are executed and reviewed.

B. SERVICE CONTINUITY MANAGEMENT POLICY STATEMENTS

1. Backups of all essential electronically maintained County business data shall be routinely created and properly stored to ensure prompt restoration.
2. Each department and/or contractor shall implement and document a backup approach for ensuring the availability of critical application databases, system configuration files, and/or any other electronic information critical to maintaining normal business operations within the department.

3. The frequency and extent of backups shall be in accordance with the importance of the information and the acceptable risk as determined by each department.
4. Departments and/or contractors shall ensure that locations where backup media are stored are safe, secure, and protected from environmental hazards. Access to backup media shall be commensurate with the highest level of information stored and physical access controls shall meet or exceed the physical access controls of the data's source systems.
5. Backup media shall be labeled and handled in accordance with the highest sensitivity level of the information stored on the media.
6. Departments and/or contractors shall define and periodically test a formal procedure designed to verify the success of the backup process.
7. Restoration from backups shall be tested initially once the process is in place and periodically afterwards. Confirmation of business functionality after restoration shall also be tested in conjunction with the backup procedure test.
8. Departments and/or contractors shall retain backup information only as long as needed to carry out the purpose for which the data was collected, or for the minimum period required by law.
9. Alternate storage facilities shall be used to ensure confidentiality, integrity and availability of all County systems.
10. Each department and/or contractor shall develop, periodically update, and regularly test business continuity and disaster recovery plans in accordance with the County's Business Continuity Management Policy.
11. Departments and/or contractors shall review and update their Risk Assessments (RAs) and Business Impact Analyses (BIAs) as necessary, determined by department management (annually is recommended). RAs include department identification of risks that can cause interruptions to business processes along with the probability and impact of such interruptions and the consequences to information security. A BIA establishes the list of processes and systems that the department has deemed critical after performing a risk analysis.
12. Continuity plans shall be developed and implemented to provide for continuity of business operations in the event that critical IT assets become unavailable. Plans shall provide for the availability of information at the required level and within the established Recovery Time Objective (RTO) and their location, as alternate facilities shall be used to maintain continuity.
13. Each department and/or contractor shall maintain a comprehensive plan document containing its business continuity plans. Plans shall be consistent, address information security requirements, and identify priorities for testing and maintenance. Plans shall be prepared in accordance with the standards established by the County's Business Continuity Management Policy.

14. Each department and/or contractor shall define failure prevention protocols to maintain confidentiality, integrity and availability. Departments shall automate failover procedures where applicable and maintain adequate (predictable) levels of ancillary components to meet this provision.