

EXHIBIT E: SECURITY AND DATA PROTECTION

DCC SECURITY AND DATA PROTECTION

DCC Security and Data Protection

The Contractor shall ensure that all software, implementation services, and related activities comply with applicable federal and State of California security standards, frameworks, and practices. The Contractor shall certify compliance to the State and maintain such compliance for the duration of the Agreement. At a minimum, the Contractor shall:

1. Governance and Accountability

1. Assume responsibility for the confidentiality, integrity, and availability of State data under its control.
2. Implement and maintain appropriate administrative, physical, technical, and procedural safeguards to prevent unauthorized access, disclosure, alteration, destruction, loss, or disruption of State data, including protection against viruses, malware, disabling devices, and other malicious or inadvertent acts that could disrupt the State's access to its data or affect the integrity of that data.
3. Comply with all statewide policies, standards, and laws regarding the use and protection of State information assets, including the prohibition on unauthorized use of data by the Contractor or third parties.
4. Require all personnel assigned under this Agreement to sign a Security and Confidentiality Statement.
5. Conduct background checks on all Contractor personnel with access to State data and ensure such personnel complete annual security and privacy training.
6. For cloud-hosted solutions, maintain certification under the Federal Risk and Authorization Management Program (FedRAMP) at a moderate or higher impact level, and provide proof of certification upon request and at no additional cost.
7. Ensure that any subcontractors or third parties engaged by the Contractor that may access, process, or store State data comply with the same requirements as the Contractor, and remain fully responsible for their performance.
8. Require disclosure of all subcontractors and sub-processors with access to State data and obtain prior written approval from the State before adding or changing any sub-processor.

2. Security Standards and Practices

1. Ensure compliance with:
 - California State Administrative Manual (SAM) Sections 5100 and 5300 through 5399
 - For cloud-hosted systems, California Statewide Information Management Manual (SIMM) 5315-B Cloud Computing Standards
 - The applicable NIST Special Publication 800-53, Revision 5 baseline controls corresponding to the system rating assigned by the State, together with any additional control enhancements

prescribed by the State

- The Criminal Justice Information Services (CJIS) Security Policy, Practices, and Procedures, for any system the State designates as subject to CJIS compliance
 - Open Worldwide Application Security Project (OWASP) secure coding and application security requirements
 - Implementation of a secure development lifecycle (SDLC) including code review, vulnerability scanning, and testing of all changes prior to production deployment
 - Conduct annual penetration testing and quarterly vulnerability scans of systems handling State data, and provide sanitized results to the State upon request
 - The State reserves the right to conduct its own security assessment or designate a third party to perform testing, with reasonable coordination from the Contractor
2. Encrypt all confidential, sensitive, or personal information, including data at rest and in transit, using end-to-end encryption methods that meet the latest FIPS cryptographic standards and in accordance with SAM 5350.1 and SIMM 5305-A.
 3. Apply security patches and upgrades, and keep anti-virus and malware protection software current on all systems used to store, process, or transmit State data.
 4. Ensure that the Contractor's primary and backup data centers where State data is stored are physically located within the continental United States, unless otherwise designated by the State.
 - 4.1 Contractor must disclose physical hosting locations and subcontracted cloud providers.
 - 4.2 Contractor must notify the State prior to any change in hosting location.
 5. Prohibit remote access to State data from outside the continental United States unless expressly authorized in writing by the State.
 6. Ensure logical or physical segregation of State data from that of other customers in any multi-tenant environment.
 7. Contractor shall not use State data for training artificial intelligence (AI) or machine learning (ML) models, product development, analytics, or any other purpose not expressly authorized in writing by the State.

3. Incident Response and Liability

1. Immediately notify the State data owner of any actual or suspected security incident involving State data.
 - 1.1 Notification shall occur no later than twenty-four (24) hours after discovery of an actual or suspected incident.
2. Cooperate fully with the State in investigating security incidents, including providing reasonable access to security logs, latency statistics, and other related information at no cost. The State reserves the right to conduct an independent investigation.
 - 2.1 The Contractor shall preserve all relevant evidence, maintain proper chain-of-custody procedures, and cooperate with the State or its designated forensic investigators during the incident response process.
3. Be responsible for all costs incurred by the State as a result of any security incident caused by the Contractor's failure to perform or the negligent acts of its personnel, including but not limited to notification, credit monitoring, staff time, material costs, postage, and media announcements.

3.1 In addition to the costs above, the Contractor shall be responsible for any regulatory fines, penalties, and breach remediation costs arising from its failure or negligence.

4. Immediately report to the State any loss or breach of data. If the State determines that notice to affected individuals is required, the Contractor shall bear all costs of notification and mitigation.
5. Immediately notify and work cooperatively with the State to respond correctly and in a timely manner to Public Records Act requests involving State data.
6. Provide the State with copies of the Contractor's most recent penetration test results, SOC 2 Type II report, or equivalent independent security assessment upon request.
7. Maintain cyber liability insurance coverage with minimum limits of five million dollars (\$5,000,000) per occurrence. Such coverage shall include, at a minimum, breach notification, credit monitoring, regulatory fines, and third-party liability arising from a security or privacy incident. Proof of coverage shall be provided to the State upon request.

4. Data Retention and Disposal

1. 4.1 Dispose of State data only as directed by the State. Data shall not be copied, modified, destroyed, or deleted other than for normal operation or maintenance, and only with prior written approval by the State.
2. Upon expiration or termination of the Agreement, return all State data to the State in a mutually agreed, readily usable format at no additional cost, and certify secure destruction of all remaining copies.
3. Contractor shall provide transition assistance to the State for a period of thirty (30) to ninety (90) days following expiration or termination, as directed by the State, to ensure orderly migration of data and services. The Contractor shall not impose excessive or unreasonable fees for data migration or transition support to the State or a successor vendor.

5. Continuity of Operations

1. Maintain documented business continuity, disaster recovery, and data backup plans to ensure timely restoration of State data and services in the event of an outage or disaster.
2. Test continuity and recovery plans at least annually, and provide test results to the State upon request.

6. Successor Standards

1. The Contractor shall comply with any successor or updated versions of the standards, policies, and frameworks identified in this Agreement, including but not limited to NIST publications, FIPS, SAM, SIMM, FedRAMP, and CJIS. Compliance with such successor standards shall occur no later than twelve (12) months after the date of their official publication, unless otherwise directed by the State.