ATTACHMENT 3

CDT-General-Terms-and-Conditions-2021

CDT Service Catalog
General Terms and Conditions

This Agreement contains the terms and conditions under which you, the Customer, agree to obtain services from the California Department of Technology (CDT). By submitting a Service Request through the CDT IT Services Portal - ServiceNow, you consent to this Agreement.

I. Service Information

The Department of Technology provides information technology services to state, county, federal and local government entities throughout California.

a. Service Catalog

The Service Catalog provides an overview of services offered by the Department of Technology.

b. CDT IT Services Portal - ServiceNow

The CDT IT Services Portal - ServiceNow is used by the Customer to request new services, modify existing services, or discontinue a service.

c. Account Lead

The Account Lead acts as the single point of contact for the Customer. The Account Lead reviews the Service Request and associated documents with the Customer to ensure the proper forms and approvals are completed. The Customer can locate their Account Lead information in the Customer Account Lead Lookup directory.

II. Service Rates

The rates charged for services under this Agreement are located in the Billing Rate Schedule. Rates are subject to change upon 30 calendar-day prior written notice from the Department of Technology. The costs for services shall be computed in accordance with the State Administrative Manual (SAM) Section 8752 and 8752.1.

III. Authority to Enter into Agreement

The Customer hereby warrants and represents that it has the budget and project approvals necessary for the services covered under this Agreement. The Customer further warrants and represents that sufficient monies are available to the Customer to fund the expenditures for services covered under this Agreement. The Customer acknowledges that it is acting in an independent capacity in making this Agreement, and not as agents or employees of the Department of Technology.

IV. Customer Invoices

Invoices shall be available by the 10th business day of the following month. The Customer will be notified by email when monthly invoices are available for viewing on the California Department of Technology Billing System (CalTABS).

V. Payment

Upon receipt of appropriate invoices for services rendered, the Customer agrees to pay the Department of Technology for actual expenditures incurred in accordance with the rates specified in the Billing Rate Schedule. The Customer further agrees to pay invoices by Direct Transfer in accordance with Government Code Section 11544(c). For Customers not required to be on the Direct Transfer program, payment is due 30 calendar days after receipt of invoice.

VI. Proprietary Rights

Pursuant to Executive Order S-16-04 and SAM Section 4846 et seq., the Customer acknowledges that the use of licensed products in violation of a valid licensing agreement could subject the Department of Technology to third-party lawsuits. The Customer, therefore, agrees that it will not duplicate, copy, or otherwise reproduce any proprietary software products supplied pursuant to this Agreement without the express written consent of the owner of the software. The Customer further agrees that it will use any such software products in strict compliance with the terms of any license provided by the owner of the software. The Customer further agrees that its use of any such licensed software products will not violate any applicable copyright, trademark, trade name, patent or similar legal right.

In the event the Department of Technology is sued by a third-party as a result of the Customer's misuse of any proprietary materials or products supplied under this Agreement, the Customer agrees to indemnify, defend and hold harmless the Department of Technology from any and all claims and losses regarding the Customer's violation of software licenses, copyrights, trademarks, trade names or any proprietary data, information or materials designated as confidential and supplied under this Agreement. If litigation arises as a result of the Customer's breach of these obligations, the Customer will pay all litigation expenses, including reasonable attorney and expert witness fees (as permitted by law), incurred by the Department of Technology in defense or settlement of the legal action or proceeding.

VII. Unsupported Software

The Department of Technology is not responsible for license, service, and/or support issues related to software in the Customer systems, unless the Department of Technology is the licensee of the software products. The Customer agrees to maintain appropriate licenses and service and support arrangements for the systems or applications owned or maintained by the Customer's department; all enterprise-wide systems, which include hardware and operating systems; application software (if applicable); security systems; and software licenses for all systems and services. The Department of Technology is neither responsible nor liable for damages resulting from the Customer's decision to use unlicensed or unsupported software.

VIII. Examination and Audit

In accordance with Government Code Section 8546.7, the Department of Technology and the Customer agree that the Bureau of State Audits (BSA) or other entity will have the right to review, obtain and copy all records pertaining to performance of this Agreement. The Department of Technology and the Customer agree to provide, or otherwise make available to, the BSA or other entity any relevant information requested and shall permit the BSA or other entity access to its premises, upon reasonable notice, during normal business hours for the purpose of interviewing employees and inspecting and copying such books, records, accounts

and other material that may be relevant to this Agreement. The Department of Technology and the Customer further agree to maintain such records for a period of three (3) years after final settlement under this Agreement.

IX. Information Security

Information Security Based on the specific requirements of SAM Section 5300 et seq., and pursuant to Government Code Section 11549.3, every state agency, department, and office shall comply with the information security and privacy policies, standards, and procedures issued by the California Information Security Office.

a. Requirements on Customer

Information security is defined as the protection of information and information systems, equipment, and people from a wide spectrum of threats and risks. To ensure the confidentiality, integrity, and availability of its managed resources, the Department of Technology agrees to provide protection of its information assets by establishing appropriate administrative, operational and technical policies, standards, and procedures. To further protect and minimize risk to the State, the Customer requesting to use the network or resources of the Department of Technology must comply with basic security requirements. By submitting a Service Request, the Customer agrees to ensure that:

1. The Customer is in compliance with statewide policies and laws regarding the use and protection of information resources and data.
2. The Customer's virus software is up-to-date and security patches and upgrades are installed on all systems on which the data may be used.
3. The Customer promptly notifies the Department of Technology Information Security Officer (ISO) of any security incidents involving information systems or data on any managed service by the Department of Technology.
4. The Customer transmitting data through resources at the Department of Technology has at least one firewall system properly situated between the network and each external entry point.
5. Physical access to network components, servers, and data storage used in conjunction with access to information resources at the Department of Technology are limited to the appropriate designated staff responsible for implementing and maintaining the components.
6. The Customer's administrative access is limited to those individuals that require access to perform duties essential to the operation and maintenance of that system.

b. Provisions provided by the Department of Technology

The California Department of Technology (hereinafter referred to as the "Department") "shall comply with applicable industry standards and guidelines, including but not limited to relevant security provisions of the California State Administrative Manual (SAM), California Statewide Information Management Manual (SIMM), The National Institute of Standards and Technology (NIST) 800-53 v4 and Federal Information Processing Standard (FIPS) Publication 199 which protect and minimize risk to the State. At a minimum, provision shall cover the following:

1. The Department will protect the confidentiality, integrity, and availability of the data under its custodianship. The Department shall implement and maintain appropriate

administrative, physical, technical, and procedural safeguards during the term of the Agreement to secure such data from data breach or loss, protect the data and information assets from breaches, introduction of viruses, disabling of devices, malware and other forms of malicious or inadvertent acts that can disrupt the State's access to its data or affects the integrity of that data.

2. Confidential, sensitive, or personal information shall be encrypted in accordance with SAM 5350.1 and SIMM 5305-A as directed by the Customer.

3. The Department shall comply with statewide policies and laws regarding the use and protection of information assets and data. Unauthorized use of data by the Department or third parties will not be allowed.

4. Signed Security and Confidentiality Statement for all personnel assigned during the term of the Agreement.

5. Apply security patches and upgrades and keep virus protection software up-to-date on all information assets on which data may be stored, processed, or transmitted.

6. The Department shall notify the State data owner immediately if a security incident involving the information asset occurs.

7. The State data owner shall have the right to participate in the investigation of a security incident involving its data or conduct its own independent investigation. The Department shall allow the Customer reasonable access to security logs, latency statistics, and other related security data that affects this Agreement and the State's data.

8. The Department shall be responsible for all costs incurred by the Customer due to security incident resulting from the Department's failure to perform or negligent acts of its personnel, and resulting in an unauthorized disclosure, release, access, review, destruction; loss, theft or misuse of an information asset. If the Department experiences a loss or breach of data, the Department shall immediately report the loss or breach to the Customer. If the Customer data owner determines that notice to the individuals whose data has been lost or breached is appropriate, the Department will bear any, and all costs associated with the notice or any mitigation required by law. These costs include, but are not limited to, staff time, material costs, postage, media announcements, and other identifiable costs associated with the breach or loss of data.

9. The Department shall immediately notify and work cooperatively with the State data owner to respond timely and correctly to public records act requests.

10. The Department shall dispose of records of State data as instructed by the Customer during the term of this agreement. No data shall be copied, modified, destroyed, or deleted by the Department other than for normal operation or maintenance during the Agreement period without prior written notice to and written approval by the Customer.

11. Remote access to data from outside the territorial United States, including remote access to data by authorized support staff in identified support centers, is prohibited unless approved in advance by the Customer.

12. The physical location of the Department data center where the Data is stored shall be within the territorial United States.

X. Limitation of Liability

The Department of Technology's liability for damages resulting from any cause shall be limited to the monthly invoice amount of the specific service impacted, except as follows:

a. The Department of Technology shall not be liable for any activity involving the Customer's installation of the product, the Customer's use of the product, or the results obtained from such use.

b. The Department of Technology shall not be liable for any unauthorized access to Customer data or any unauthorized disclosure of Customer data resulting from the Customer's use of any product.

c. In no event shall the Department of Technology be liable to the Customer for consequential damages, even if notification has been given as to the possibility of such damages.

XI. Changes to Service

All notices relating to changes, additions, or modifications of service shall be in writing and shall be submitted by the Customer through the CDT IT Services Portal - ServiceNow.

No variation of the terms of the service shall be valid unless made in writing, signed by the Department of Technology and the Customer, approved as required, and submitted through the CDT IT Services Portal - ServiceNow. No verbal understanding or agreement is binding on any of the parties.

XII. Disputes

In the event of a dispute, the Department of Technology shall continue with the responsibilities of providing services to the Customer.

XIII. Problem Escalation

The Customer acknowledges and agrees that certain technical and project-related problems or issues may arise, and that such matters shall be promptly reported to the Department of Technology. The Department of Technology agrees to provide an internal escalation process to facilitate communication between the Customer and staff at the Department of Technology, as appropriate. The Account Lead will determine the problem severity level, and notify appropriate staff at the Department of Technology including, but not limited, to the following:

First Level	Section or Unit Manager/Service Owner
Second Level	Branch Chief/Service Owner
Third Level	Division Deputy Director

XIV. Cancellation of Service

The Customer must provide 45 calendar days cancellation notice for a service to be terminated. Cancellation of services is vendor-dependent and may require lead-time for processing termination documents. The Customer must submit a Service Request through the CDT IT Services Portal - ServiceNow to notify the Department of Technology of the intent to terminate services. The targeted completion date noted on the Service Request must allow for the lead-time required to cancel services. Retroactive termination of services will not be considered. For more information regarding lead- times for canceling services, please contact your Account Lead.