

Dist. *IT* *Cleared*
CSG *5/3/2021*

STATE OF CALIFORNIA - DEPARTMENT OF GENERAL SERVICES

STANDARD AGREEMENT

STD 213 (Rev. 04/2020)

AGREEMENT NUMBER

M63734-7100

PURCHASING AUTHORITY NUMBER (If Applicable)

EDD-7100

1. This Agreement is entered into between the Contracting Agency and the Contractor named below:

CONTRACTING AGENCY NAME

Employment Development Department

CONTRACTOR NAME

Accenture LLP

2. The term of this Agreement is:

START DATE

February 4, 2021

THROUGH END DATE

February 3, 2022

3. The maximum amount of this Agreement is:

\$10,575,000.00

Ten Million Five Hundred Seventy-Five Thousand and Zero Cents

4. The parties agree to comply with the terms and conditions of the following exhibits, which are by this reference made a part of the Agreement.

Exhibits	Title	Pages
Exhibit A	Statement of Work	15
Attachment A-1	Cyber Defense Supplement	2
Attachment A-1, Exhibit I	Data Privacy and Security	2
+ Attachment A-1, Exhibit II	Data Safeguards for Client Data	6
+ Attachment A-2	Remote Work Protocols	2
+ Attachment A-3	AIP + Addendum	2
+ Attachment A-3, Exhibit A	Terms and Conditions	3
+ Attachment A-3, Exhibit B	Cloud Services Vendor Terms	1
+ Attachment A-3, Exhibit C	Data Processing and Security Terms	3
+ Exhibit B	Budget Detail and Payment Provisions	2
+ Attachment B-1	Costs	1
+ Exhibit C	GTC 04/2017 - As Modified	6
+ Exhibit D	Protection of Confidentiality	3
+ Attachment D-1	Confidentiality Agreement	1

STATE OF CALIFORNIA - DEPARTMENT OF GENERAL SERVICES

STANDARD AGREEMENT

STD 213 (Rev. 04/2020)

AGREEMENT NUMBER

M63734-7100

PURCHASING AUTHORITY NUMBER (If Applicable)

EDD-7100

Exhibits	Title	Pages
+ Attachment D-2	Idemnity Agreement	1
+ Attachment D-3	Statement of Responsibility	1
+ Exhibit E	Safeguarding Contract Language Administrative Requirements	2
+ Exhibit F	Safeguarding Contract Language For Technology Services	3
+ Exhibit G	Special Terms and Conditions	4

Items shown with an asterisk (*), are hereby incorporated by reference and made part of this agreement as if attached hereto.

These documents can be viewed at <https://www.dgs.ca.gov/OLS/Resources>

IN WITNESS WHEREOF, THIS AGREEMENT HAS BEEN EXECUTED BY THE PARTIES HERETO.

CONTRACTOR

CONTRACTOR NAME (if other than an individual, state whether a corporation, partnership, etc.)

Accenture LLP

CONTRACTOR BUSINESS ADDRESS

CITY

STATE

ZIP

PRINTED NAME OF PERSON SIGNING

TITLE

CONTRACTOR AUTHORIZED SIGNATURE

DATE SIGNED

April 30, 2021

STATE OF CALIFORNIA

CONTRACTING AGENCY NAME

Employment Development Department

CONTRACTING AGENCY ADDRESS

CITY

STATE

ZIP

PRINTED NAME OF PERSON SIGNING

TITLE

CONTRACTING AGENCY AUTHORIZED SIGNATURE

DATE SIGNED

May 3, 2021

CALIFORNIA DEPARTMENT OF GENERAL SERVICE

EXEMPTION (If Applicable)

Exempt per Governor's Proclamation of a State Emergency, effect March 4, 2020 (GC Sections 8625-8629)

EXHIBIT A
(Standard Agreement)
Statement of Work

1. PURPOSE

The purpose of this Contract is to acquire Contractor resources to perform fraud consulting services (the "Services") for the California Employment Development Department ("EDD" or the "State" or "Client"). Accenture LLP (the "Contractor" or "Accenture") will provide advisory services, including, but not limited to, fraud analysis, fraud data analytics, review of policies, cybersecurity assessment, and assistance in resolving State of California Auditor recommendations, on behalf of and at the direction of the EDD, all as set forth more fully below.

2. PERIOD OF PERFORMANCE

The term of this Contract shall begin on the date specified on the STD 213 Cover page and end 12 months later. The State may, at its sole discretion, elect to extend the Contract term as needed for up to 2 additional 12-month terms, at the hourly rates described in Attachment B-1, Standard Agreement Costs, which extensions shall not be denied by the Contractor (each an "Extension"). However, the State is not obligated to use any or all of these Extensions.

On February 4th, 2021, the Contractor received written direction from the EDD to commence Services (as later defined) under this Contract.

3. AMOUNT OF CONTRACT

The total price of this Contract is the amount contained on the STD 213 cover page. Cost details are further described in the Costs, Attachment B-1. In no event shall the total amount of the Contract exceed the amount contained on the STD 213 cover page, and there is no obligation on the part of the EDD to utilize the entire amount or obligation on the part of the Contractor to continue performing the Services once the total amount is reached absent an Amendment executed in accordance with this Contract. In the event that any systems or products not specified in this Contract are deemed to be needed by both EDD and Contractor to perform services herein, the parties shall select the appropriate systems or products and decide on cost and integration responsibilities at that time.

4. WORK LOCATIONS/HOURS

Employees of the Contractor ("Consultant(s)") are able to perform Services up to a full-time basis and are permitted to work remotely in accordance with Attachment A-2. Travel is not required and will not be requested. The Contractor will not be reimbursed for any travel costs unless approved in advanced by the EDD. Full-time equivalent (FTE) is estimated to be a minimum of 2080 hours annually or 40 hours per work week per Consultant. Core business hours are Monday through Friday, 8 a.m. to 5 p.m., apart from State Holidays. The Consultants may be required to provide support beyond the normal core business hours.

**EXHIBIT A
(Standard Agreement)
Statement of Work**

For all work hours, the Contractor will be paid at the same hourly rate indicated in Attachment B-1, Cost Table.

"Offshoring" of work performed under this Contract is prohibited, unless mutually agreed to by the parties.

5. DESCRIPTION OF SERVICES

The Contractor shall work with the EDD to assess EDD's fraud detection and prevention capabilities and provide advisory services in support of resolving certain audit recommendations from the California State Auditor. In addition, the Contractor shall provide cybersecurity assessments as set forth in the Service Domains in Section 7. The Contractor resources will work collaboratively and directly with the State's Directorate and Executive team, EDD's Policy, Accountability and Compliance Branch (PACB), Project Managers, Program Managers, Functional Managers, and/or technical staff.

SCOPE OF WORK

As the EDD seeks to identify opportunities to improve its fraud program and ultimately benefit claimants and taxpayers, it seeks a comprehensive review across its fraud management and prevention capabilities.

Working collaboratively with EDD, Contractor will advise and assist the EDD across the following service domains (collectively the "Service Domains" and each a "Service Domain"):

1. Fraud Organization Design Support
2. California State Auditor Remediation Assistance for
 - a. State of California Auditor (CSA) Report: 2020-128/628.1 (Issued: January 26th, 2021)
 - b. State of California Auditor (CSA) Report: 2020-628.2 (Issued: January 28th, 2021)
3. Cybersecurity Support
4. PMO

The Contractor will share information across the Service Domains to support effective knowledge sharing and alignment with the EDD. This parallel execution approach will focus on both tactical, shorter-term support, such as assistance in remediating certain state auditor findings and advising on the mitigation of more immediate threats, and more strategic efforts, such as advising on changes to organizational structure and policy for the EDD's fraud organization. Contractor will also refer to relevant National Association of State Workforce Agencies (NASWA), Government Accountability Office (GAO), and other regulatory guidelines to inform its approach for this engagement as directed by the EDD.

**EXHIBIT A
(Standard Agreement)
Statement of Work**

CHANGES OF SCOPE

Any change of scope will require a written change order notification provided in advance and will be subject to mutual agreement between Contractor and the EDD.

6. WORK ACCEPTANCE CRITERIA

The EDD shall be the sole judge of the acceptability of all tasks and services performed by the Contractor as a result of the Contract. Should the work performed, or service or tasks performed by the Contractor, fail to meet the minimum EDD conditions, requirements, applicable standards, specifications, or guidelines, as stated in writing or defined herein, the following resolution process will be employed, except as superseded by other binding processes:

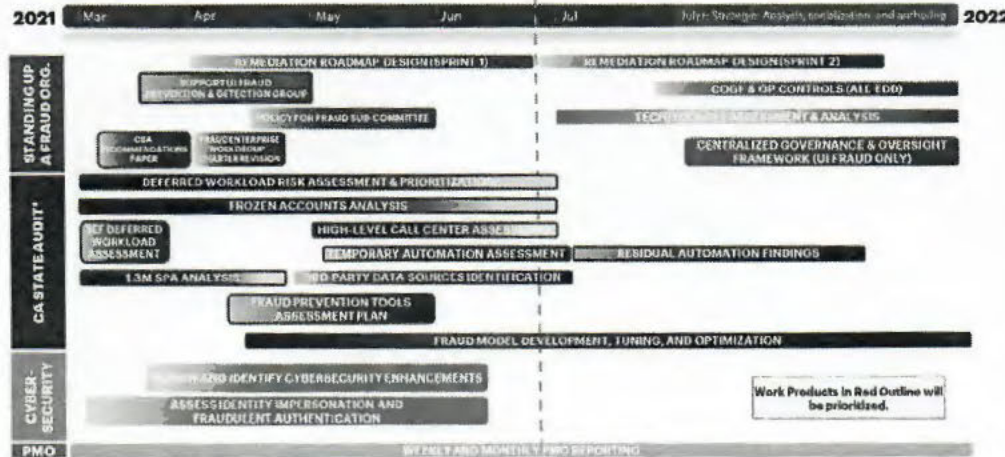
- a) The EDD shall notify the Contractor in writing, within five business days after completion of services, of any acceptance problems by identifying the specific inadequacies and/or failures in the services or tasks performed by the Contractor. The Contractor will produce work products as suggested in Table A – Indicative Work Products in Section 7 and the review criteria would include clarity in documentation of observations from the listed Service Domains in section 7.
- b) The Contractor shall, within five business days after initial problem notification, respond to the EDD by submitting a detailed description of how the identified services and/or work product actually adhere to applicable requirements, as mentioned above, and/or a proposed corrective action plan to address the specific inadequacies in the identified services and/or work product.
- c) The EDD shall, within five business days after receipt of the Contractor's detailed explanation and/or proposed corrective action plan, notify the Contractor in writing whether it accepts or rejects the explanation and/or plan. If the EDD rejects the explanation and/or plan, the Contractor will submit a revised corrective action plan within three business days of notification of rejection.
- d) The EDD shall, within three business days of receipt of the revised corrective action plan, notify the Contractor in writing whether it accepts or rejects the revised corrective action plan proposed by the Contractor.

7. CONTRACTOR TASKS AND SERVICES

Contractor will advise and assist EDD in its efforts on a time-and-materials basis through the following tasks and services.

PROJECTED WORKING TIMELINE

EXHIBIT A (Standard Agreement) Statement of Work



The timeline through June 30, 2021 shown above depicts how Contractor plans to dedicate its resources in support of EDD. As the services are performed in the Service Domains during the initial four months of the project (and continue beyond in certain cases), Contractor and EDD will collaborate and agree on the allocation of resources to specific initiatives for the remainder of the Contract term no later than June 30, 2021. This agreement will be documented via a mutually executed Work Authorization, or Contract Amendment, as applicable, no later than June 30, 2021.

SERVICE DOMAINS

1. Fraud Organization Design Support

Contractor will work closely with EDD resources to support EDD's understanding and development of organizational capabilities required to mitigate the risk of unemployment insurance fraud. To do so, Contractor will collaborate with EDD resources to perform the following services:

- a) Advise and assist the EDD with the establishment of a Fraud Working Group through advising upon an initial charter that establishes roles and responsibilities, cadence, and governing principles.
- b) Advise the EDD in the evolution of an unemployment insurance (UI) Fraud Working Group Sub-committee by assisting with its Recommendations Paper to the California State Auditor (CSA) due at the end of March 2021.
- c) Co-develop with EDD an organizational policy for UI-related fraud sufficient to meet the EDD's objective, roles & responsibilities, paths for escalation, and governance / oversight.
- d) Assist the EDD with design considerations for its future-state organizational structure in support of its organizational policy for UI fraud.

EXHIBIT A
(Standard Agreement)
Statement of Work

- e) Assist the EDD with identifying opportunities to improve the current state of the EDD Fraud Organization against a reference capability model for fraud prevention and detection.
 - f) Assist EDD in its efforts to identify, analyze and rank-prioritize opportunities for the development of EDD fraud management capabilities; these capabilities will be laid out in strategy and roadmap.
2. Data and Analytics Advisory Services in Support of CA State Auditor Remediation Activities
- Contractor will work closely with EDD resources to assist the EDD with addressing certain California State Auditor Recommendations indicated in the list below. To do so, Contractor will collaborate with EDD resources to perform the following services:
- a) Assist the EDD in the resolution of State of California Auditor (CSA) Report 2020-628.2 recommendation #5, supporting the EDD's assessment of frozen / blocked claimant card accounts at Bank of America accounts as related to risk associated with possible fraudulent claims.
 - b) Work with the EDD to identify, categorize, and document the risks associated with possible UI fraud within with the existing deferred workload population [CSA Rec. #5, 2020-128/628.1].
 - c) Support the EDD on a fraud risk-driven prioritization of the deferred workload population based on UI fraud risk ratings [CSA Rec. #6, 2020-128/628.1].
 - d) Assist with the formation of a plan for the EDD to assess the effectiveness of its fraud prevention tools [CSA Rec. #9, 2020-628.2].
 - e) Assist the EDD with the high-level review of the EDD's call center as it relates to unemployment insurance fraud.
 - f) Assist with the retrospective analysis regarding unemployment insurance claims related to the California School Employer Fund (SEF) submitted in calendar year 2020.
 - g) Assist with the analysis of approximately 1.3M UI claims [of a population of 1.4M UI claims flagged for fraud] filed in the year 2020 that 1) triggered stop payment alerts (SPA) for issues related to suspected identity-related fraud and 2) did not respond to EDD requests for more information prior to disqualification.
 - h) Help the EDD analyze which of the EDD's temporary automation measures for claims processing can be retained and assist with a final designation of permanent claims processing features [CSA Rec. #3, 2020-128/628.1].
 - i) Support the EDD in the selection of third-party data resources to augment the EDD's fraud prevention and detection capabilities.
 - j) Provide findings about opportunities to increase the fraud capture rate and decrease false positives in a scalable way to manage periods of high UI benefits claims (e.g., recession) [CSA Rec. #1, 2020-628.2]. Potential areas of opportunity include measures to enhance fraud monitoring model capabilities, to develop features to increase fraud prevention and detection capabilities, and to perform model tuning and optimization procedures.

**EXHIBIT A
(Standard Agreement)
Statement of Work**

3. Cybersecurity Support

Contractor will work closely with EDD resources to conduct a cybersecurity assessment and provide recommendations for addressing the cybersecurity-related findings captured in the *Employment Development Department Strike Team Detailed Assessment and Recommendations* report published on September 16, 2020. To do so, Contractor will collaborate with EDD resources to perform the following services:

- a) Help to analyze existing security tools at EDD (functionality, coverage, and staff usability) and identify areas for improvements.
- b) Identify areas for improvement related to identity access management (IAM) enterprise architecture.
- c) Assess identity impersonation and fraudulent authentication based on EDD-provided sample logs containing cases of confirmed fraud.
- d) Perform high-level analysis on current state of identity authentication, help identify fraudulent activities in the process, and advise on specific actions to mitigate the risks.

4. Program Management Office (PMO)

Contractor will oversee and track progress of the services described in service domains 1, 2, and 3. To do so, Contractor perform the following services to give EDD transparency into progress:

- a) Provide weekly and monthly reports/updates that include accomplishments for the previous periods, future work plans, and the identification of project issues and risks.

Indicative Work-Products

The Contractor will advise and assist the EDD in producing work products. The below mentioned indicative work products are the type of work products that may be created; the parties will cooperate to determine the actual work products to be created pursuant to the project management processes. The parties acknowledge the resulting work products are created and intended for EDD's purposes only and can be shared with third parties at EDD's discretion accordance with Section 9(r)(iv) of this SOW.

EXHIBIT A
(Standard Agreement)
Statement of Work

Table A: Indicative Work Products	
Service Domain	Indicative Work Products
Fraud Organization Design Support	Fraud Working Group Charter Recommendations (Word), UI Fraud Working Group Sub-committee Recommendations Paper (Word), Draft UI Fraud Policy (Word), Fraud Organization Design Recommendations (PowerPoint), Fraud Strategy Document (PowerPoint), Remediation Roadmap (PowerPoint)
California State Auditor Remediation Assistance	Deferred workload risk assessment report (PowerPoint), School Employer Fund (SEF) Deferred Workload Assessment Report (PowerPoint / Excel), Retrospective Analysis of 1.3M Claims with Stop Payment Alerts (SPA) (PowerPoint / Excel), High-level Call Center Assessment (PowerPoint), Temporary Automation Report (Word / PowerPoint), Frozen Account Review Report (PowerPoint), Fraud Prevention Tools Assessment Report (PowerPoint)
Cybersecurity Support	Security assessment report (Word / PowerPoint), Fraudulent authentication analysis report (Word / PowerPoint)
Program Management Office (PMO)	Weekly and Monthly Status Reports (PowerPoint)

ASSUMPTIONS

- a) The EDD will make EDD personnel and its partner subject matter advisors available for assistance in a timely fashion as required by the Contractor to ensure the completion of agreed upon project timelines. Any decisions to be made by EDD will be made promptly and without delay.
- b) This SOW assumes use of the current state platforms and tools for the purposes of the assessments. The cost of additional software and tools is not included in this Contract. Contractor can provide findings and budget estimates upon further discussion and inputs such as key usage metrics and inventory of existing licenses to create, install, or use different platforms and tools if Contractor and EDD mutually agree. EDD will provide any access to such software and tools necessary for the Contractor to perform its obligations under this Contract.
- c) If access to adequate tools, products, systems, or data to perform Services is not made available in a timely manner and consumable condition, the EDD recognizes that the quality and timeliness of Services may be adversely impacted.
- d) In the event that a Contractor is exposed to data that identifies or directly relates to natural persons as may be further defined in applicable data privacy law ("Personal Data") during the performance of this SOW, Contractor will follow the protocols outlined in Attachment A-1, A-2, and A-3.
- e) EDD has already begun developing the fraud working group governance with regards to fraud prevention and detection; any artifacts will be used by the Contractor to build upon and refine in collaboration with designated EDD personnel in support of advisory services provided for under Service Domain 1.

EXHIBIT A
(Standard Agreement)
Statement of Work

- f) Revision and socialization of the fraud strategy document under Service Domain 1 will take place in no more than three (3) working sessions with designated EDD personnel.
- g) The Contractor will run no more than one (1) working session with designated EDD personnel to define and decide on the prioritized remediation roadmap under Service Domain 1.
- h) An EDD designee will be assigned to own and lead the remediation project plan while being advised and assisted by the Contractor.
- i) EDD will provide feedback on and lead any installation efforts related to 3rd party data sources identified by Contractor in support of Service Domain 2.
- j) EDD will provide designated personnel to dedicate to a weekly working session to co-assess and co-develop the high-level call center assessment. Infrastructure management including network, security, compliance management, and hardware changes will be handled by EDD.
- k) EDD will provide detailed information regarding fraud models being considered for testing and those in production to support Service Domain 2, including, but not limited to, access to source data/systems, subject matter resource time, model development and deployment process documentation, model repository (e.g., model registry), and historical analyses/forecasts of fraudulent claims.
- l) No more than two fraud models will be tuned and operationalized by the Contractor as a result of activity performed in support of Service Domain 2.
- m) EDD will provide any and all access required to tune and operationalize prioritized fraud models in a development environment to support Service Domain 2.
- n) The Contractor and its personnel are not licensed to, do not provide, and will not be required to provide any legal, regulatory, audit, accounting, tax, or similar professional advice. EDD will be responsible for obtaining such advice from its own legal counsel or other licensed professionals, who will review, supervise, and approve any relevant Services and work product.
- o) The Contractor and its affiliates perform various consulting, technology and operations services for many government and commercial clients within and outside of the State of California that could potentially be impacted by guidance or services provided by the Contractor as part of the Services provided hereunder. Accordingly, there may be a perception of an organizational conflict of interest between such services and the Services provided hereunder. The Contractor has established and will maintain reasonable safeguards, including personnel assignment and confidentiality controls to help avoid any actual organizational conflict of interest and to help ensure that its personnel do not use their positions or information learned in the course of performing the requested services for any purpose outside of these Services. Subject to such safeguards, EDD acknowledges that the provision of Services hereunder does not constitute an organizational conflict of interest for the Contractor.
- p) The Contractor shall not independently validate any information provided to it by EDD, its agents or third parties, and shall be entitled to rely upon such information.

EXHIBIT A
(Standard Agreement)
Statement of Work

- q) EDD has obtained all consents necessary from third parties required for the Contractor to perform its obligations hereunder, and EDD will be responsible for the contractual relationship with and performance of such third parties as required.
- r) EDD will be responsible for ensuring that consent is obtained from individuals to share any data with the Contractor and for its use in connection with the Services.
- s) The Contractor accepts no responsibility for the accuracy or integrity of any data provided in connection with the Services nor will it verify the accuracy or integrity of such data.
- t) Any Personal Data will be maintained on EDD's systems or within an alternate external environment, as mutually agreed to by the EDD and Contractor. [See Attachment A-3]

8. CONTRACTOR RESPONSIBILITIES

The Contractor shall:

- a) Designate a person to whom all service or project related communications may be addressed;
- b) Meet regularly with EDD personnel to discuss required activities;
- c) Provide a weekly status report, by Tuesday of each week, that documents tasks/assignments and includes that include accomplishments for the previous periods, future work plans, and identification of any issues/risks;
- d) Provide a monthly status report, by the fifth calendar day of each month, that documents tasks/assignments and includes that include accomplishments for the previous month, future work plans for the coming month, and identification of any issues/risks;
- e) Comply with all applicable EDD policies and procedures, including, but not limited to, the EDD and industry project management guidelines, as provided by EDD to Contractor in writing in advance;
- f) Advise and assist in project management, quality management, change control, communication management, risk and issue management, and scheduling of management tasks/assignments as required;
- g) Provide all electronic documents to EDD in a format compatible with EDD's standard applications (i.e., Microsoft (MS) Office). EDD's current standard applications include MS Windows 10, MS Office Professional (includes Outlook) 2013, Visio 2013, Project 2013;
- h) Verify that its applications are compatible prior to delivery of any electronic documents to EDD. The EDD shall approve in writing any other format to be used by the Contractor;
- i) Agree to upgrade versions of its software, if needed, at no cost to the State in order to remain compatible with EDD's standard applications;
- j) Provide paper deliverables printed on 8½" x 11" paper, to the extent practicable;

EXHIBIT A
(Standard Agreement)
Statement of Work

- k) Post electronic documents to an EDD designated electronic repository, e.g., a SharePoint site. The electronic document format and media shall be compatible with EDD storage devices; and
- l) Return all EDD property, including security badges, prior to termination of the Contract.

9. STATE RESPONSIBILITIES

The EDD is responsible for program and policy. The following are areas of responsibility for EDD staff:

- a) **Oversight:** Oversee all aspects of the Initiatives using the EDD's Project Management Methodology.
- b) **Contract Management:** Oversee planning, solicitation, acquisition, contract monitoring, change management, and contract amendments, including managing third-party contractor activities, and ensuring a collaborative relationship with the third-party contractor.
- c) **Communication and Change Management:** Ensure communication among the EDD, Contractor personnel, and other project stakeholders; develop and manage change management processes.
- d) **Administrative Support:** Complete administrative tasks and support project management.

The EDD shall:

- a) Be responsible for oversight of development and control support activities, ensuring compliance with the CDT and Department of General Services (DGS) standards, stakeholder management, budgetary approvals, contract management, and procurement, as applicable.
- b) Make EDD personnel available for assistance in a timely fashion as required by the Contractor on a timely basis to ensure the completion of agreed upon project timelines.
- c) Facilitate access to relevant third-party personnel, resources, technology, and documentation in a timely fashion as required by the Consultant to conduct services on behalf or in support of EDD.
- d) Provide access to applicable information, including, but not limited to technical documentation and project work plans.
- e) Provide workspace including desks, chairs, telephones, personal computers, printer access, Internet connections, virtual desktop infrastructure (VDI), MS Office, and MS Project (as needed).
- f) Provide remote access to all environments and infrastructure necessary to complete services in a timely fashion and as required to meet project deadlines, through a VDI.

EXHIBIT A
(Standard Agreement)
Statement of Work

- g) Provide timely feedback and participate in socialization sessions with the Contractor on an as-needed basis to ensure prompt refinement and approval of all services.
- h) Provide timely access to data, software and systems in the EDD environment, or in an alternate external environment, as mutually agreed to by the parties, as identified, and/or as required to accomplish support activities on aforementioned Service Domains.
- i) Provide all applicable policies and procedures regarding access to, and use of, EDD facilities; provide information as required by the Contractor to perform their responsibilities.
- j) Review all Contractor work submitted to the EDD for completeness, accuracy, and adherence to standards.
- k) Make relevant and necessary EDD documentation available upon request by the Contractor in a timely manner.
- l) Provide business requirements for system changes.
- m) Conduct user testing and certify software changes for implementation.
- n) Provide the necessary environments and infrastructure to support system development and implementation.
- o) Provide required cybersecurity documentation reflecting current state of people, process, and technologies.
- p) Make available personnel to provide undocumented information for cybersecurity.
- q) Provide resources that will support identity mitigation activities.
- r) Be responsible for its operation and use of the Services and work product(s) and for determining whether the Services and work product(s) meet the EDD's requirements and comply with any laws, regulations, policies or guidance to which the EDD is subject. EDD expressly acknowledges that it is ultimately responsible for assessing the applicability and relevance of the work product, whether to take action based on the findings in any work product, and whether to implement any changes to EDD's internal policies, systems or security measures based on such work product; and (iv) whether to share any work product or portions thereof, including without limitation any of Contractor's analyses or recommendation, to any person or entity other than EDD and addressing any follow-up thereto.

10. UNANTICIPATED TASKS

Unanticipated tasks will be contracted for on an as-needed basis and shall be optional throughout the term of the Contract. Work for unanticipated tasks will be assigned and agreed to in writing by the Contractor and the EDD via a Work Authorization (WA) before the work can commence. The rates for unanticipated tasks must not exceed the hourly rates specified in Attachment B-1, Cost Table for unanticipated tasks and the total expenditures shall not exceed the total amount of the contract.

EXHIBIT A
(Standard Agreement)
Statement of Work

11. CONTRACTOR REQUIREMENTS AND REASSIGNMENT

The Contractor shall:

- a) Be responsible for monitoring the monthly hours billed to confirm that the Contractor can effectively meet the project needs. Given the scope and time constraints of this project, it is of utmost importance that Consultants have the adequate dedicated hours to perform work effectively.
- b) Maintain the sole right to determine the assignment of its Consultants that meet or exceed the requirements stated in this Contract, and to alter the configuration / composition of its team of Consultants to support the changing requirements of the project over the course of time or in response to new developments / discovery.
- c) Agree to notify the EDD in writing, as soon as is practical, of all changes in the assignment of any Consultants.
- d) Make a reasonable effort to promptly remove the Consultant and provide a suitable replacement, if the EDD reasonably determines that a Consultant is failing to adequately perform services for cause, illness, resignation, breach of security, unacceptable conduct, failure to follow EDD policies, or other factors (regardless of whether or not it is within the Contractor's control). A suitable replacement is defined as possessing the equivalent or better minimum qualifications (MQs) than the Consultant being replaced.
- e) Negotiate with EDD the hourly rate of any substitute Consultant(s) to the Contract. The hourly rate negotiated shall be dependent, in part, upon the experience and individual skills of the proposed substitute Consultant. The negotiated rate cannot exceed the hourly rate already stated in the Contract for Consultants with equivalent experience and individual skills.
- f) Maintain satisfactory standards of employee competency, conduct, appearance, and integrity.
- g) Ensure Consultant(s) do not disturb papers on desks, open desk drawers or cabinets, or use State equipment, except as authorized.

12. CONTRACTOR PARAMETERS

The Contractor will provide the independent services described by this SOW, and associated Standard Agreement (STD. 213), subject to the following:

- a) The EDD will not reimburse for any expenses incurred by the Contractor in the execution of activities except as specifically preauthorized in writing by the EDD.
- b) All data, documents, software and other work product produced under the Contract will become the sole property of EDD except for preexisting materials and all derivatives and modifications thereof, which shall remain owned by the Contractor.

EXHIBIT A
(Standard Agreement)
Statement of Work

13. USE OF SUBCONTRACTORS

The Contractor may, with the approval of the EDD Directorate and/or PACB and the BOPSD Analyst, enter into subcontracts with third parties for the performance of any part of the Contractor's duties and obligations. Any such State approval may be rescinded for reasonable cause. The Contractor is responsible and liable for the proper performance and quality of any work performed by any and all subcontractors. The State reserves the right to reject or refuse admission to State facilities to any subcontractor personnel whose workmanship, in the reasonable judgment of the State, is deemed to be substandard. In no event shall the existence of a subcontract release or reduce the liability of the Contractor to the EDD for any breach in performance of the Contractor's duties.

14. SECURITY

The Contractor shall supply the respective EDD Program Manager with the names of the Consultant(s) who are assigned to this project and will need access to EDD facilities. The Contractor shall notify the EDD Security Administrator of all changes, as soon as is practical. The EDD shall issue identification (ID) badges to each Consultant to allow them access to those areas of the building where they will be performing services. These ID badges are the property of EDD and the Consultants must surrender them when they leave the project(s) or at the end of the Contract term.

The EDD shall issue computer user accounts to each Consultant as needed and for no longer than the duration of the Contract. An Appointment/Separation Checklist (DE 7411) shall be completed for all such accounts and shall reflect the account ID and the anticipated expiration date.

The EDD Single Point of Contact (SPOC) may request that the EDD Security Administrator extend the user account ID expiration date by sending a request with a new anticipated account expiration date. EDD shall cancel user account access as soon as there is no longer a business need for such access, or when the Consultant is no longer working on the project.

The parties will comply with the provisions of Attachment A-1, Attachment A-2 and Attachment A-3.

15. INSURANCE REQUIREMENTS

Contractor agrees the insurance herein provided for shall be in effect at all times during the term of this Contract. In the event said insurance coverage expires at any time during the term of this Contract, Contractor agrees to provide, within 30 days after said expiration date, a new certificate of insurance evidencing insurance coverage as outlined below for not less than the remainder of the term of this Contract, or for a period of not less than one year. New certificates of insurance are subject to the approval of the Department of General

EXHIBIT A
(Standard Agreement)
Statement of Work

Services (DGS), and Contractor agrees that no work or services shall be performed prior to the giving of such approval or alternative approval provided by EDD. In the event the Contractor fails to keep in effect at all times insurance coverage as herein provided, the State may, in addition to any other remedies it may have, terminate this Contract upon the occurrence of such event. The Contractor shall provide written notice to EDD within five (5) business days of any cancellation, non-renewal, or material change that affects required insurance coverage.

The Contractor shall display evidence of the following coverage on an ACORD certificate:

Commercial General Liability Insurance -Contractor shall furnish to EDD a certificate of insurance prior to commencement of work stating there is commercial general liability insurance in effect for the Contractor in an occurrence form with limits not less than \$1,000,000 per occurrence for bodily injury and property damage combined.

The certificate of insurance must include the following provision stating:

The State of California, its officers, agents, employees, and servants are included as additional insured, but only with respect to work performed for EDD under this contract. *The blanket additional insured endorsement must accompany the certificate.*

16. WORKERS COMPENSATION

Workers' Compensation and Employers Liability Insurance -The Contractor shall furnish to EDD a certificate of insurance evidencing Workers' Compensation and Employers Liability Insurance presently in effect with limits not less than \$1,000,000 by an insurance carrier licensed or legally permitted to write Workers' Compensation insurance in California. Such certificate shall include the name of the carrier and the policy inception and expiration dates. If the Contractor is self-insured for Workers' Compensation, a certificate must be presented evidencing Contractor is a qualified self-insurer in the State of California.

17. CONFIDENTIALITY AND NON-DEBARMENT

In addition to the terms and conditions of the General Terms and Conditions, pertaining to confidentiality and non-debarment, the Contractor shall sign all confidentiality, non-debarment, privacy, security, conflict of interest, and other necessary agreements as required by the EDD and agreed by the Contractor to successfully provide the services described in the Contract.

**EXHIBIT A
(Standard Agreement)
Statement of Work**

All financial, statistical, personal, technical, and other data and information provided to the Contractor by the EDD, pursuant to the terms of the Contract, are confidential information pursuant to Section 1094 of the California Unemployment Insurance Code. As such, the Contractor hereby agrees to maintain and protect the confidentiality of said information and shall disclose said information to its own employees or subcontractor(s) only on a "need-to-know" basis and only for the purposes of fulfilling the terms of this Contract. In no event shall said information be disclosed to any individual other than the Contractor's employees or subcontractor(s). The Contractor further agrees to retain the confidential information for three years after final payment under the contract.

To preserve the integrity of the security and confidentiality measures integrated into EDD's automated information systems, each Consultant is required to provide a signed Employee Confidentiality Statement (DE_7410) prior to starting work.

18. TERMINATION CLAUSE

This Agreement may be terminated by either party by giving written notice 30 days prior to the effective date of such termination.

19. DISCREPANCIES

Should any error, discrepancy, or doubt arise as to the performance of the Services, the Contractor shall immediately refer the same to the EDD Representative for further instructions before proceeding with the work affected.

20. POINTS OF CONTACT

The EDD shall designate a SPOC who shall give direction to the Contractor concerning the assigned tasks. The SPOC will work collaboratively with the EDD Management Team, Program Managers, Functional Managers, and technical staff to ensure that all work products are satisfactorily completed. The SPOC shall be the Program Manager who shall ensure that all contract activities are conducted in accordance with State law and regulations; oversee processes and procedures; monitor contractor compliance with the contract; and resolve issues.

21. CYBER DEFENSE SECURITY TERMS

The parties agree that, solely with respect to the provision of security Services performed under this SOW, the supplemental terms and conditions attached hereto as Attachment A-1 shall apply.

**Attachment A-1
(Standard Agreement)
Cyber Defense Supplement**

Cyber This Cyber Defense Services Supplement (the "**Cyber Defense Supplement**") supplements and amends the terms of the Agreement No. M63734-7100 between EDD and Accenture LLP, dated February 4, 2021 (the "Agreement"), and shall apply solely to the provision of security Services set out in the Statement of Work agreed by the parties.

To the extent that the terms of this Cyber Defense Supplement conflict with the Agreement, this Cyber Defense Supplement shall prevail. To the extent to which the SOW conflicts with the terms of this Cyber Defense Supplement, then the SOW shall prevail in respect of the relevant services set out in that SOW only.

A) CONSENT AND AUTHORIZATION

Unauthorized access to computer systems or data or intrusion into hosts and network access points may be prohibited by applicable law. Client: (i) explicitly warrants that it has obtained all applicable consents and authorizations for Accenture to deliver the Services to be provided under this Agreement, as described in an applicable SOW; (ii) hereby gives Accenture explicit permission to take all actions as necessary to perform the Services and to access, and process any and all Client Property (as defined below) related to the Service, including without limitation, if applicable, consent to connect to Client's computer network, install software and/or hardware, collect and analyze host and network based data including but not limited to, memory, disk, logs, data, and historic or real time network traffic as well as any malware ("**Forensics Data**"), archive, analyze, and retain all Forensics Data captured or obtained as part of Services, circumvent or overcome technology or physical measures designed to protect against unauthorized access to Client Property, including those that effectively control access to material protected by intellectual property laws, as well as use or provide technology to achieve any such circumvention, and intercept telecommunications and electronic communications; (iii) hereby gives Accenture explicit permission to comply with the requirements of law enforcement authorities or regulatory authorities (provided, that Accenture will use reasonable endeavors to notify the Client in advance of responding to any such requirements and, if possible, will allow Client opportunity to raise an objection with such authorities); and (iv) represents and warrants that such access and processing by Accenture does not violate any applicable law or any obligation Client owes to a third party. Accordingly, Client warrants and represents that it is the owner or licensee of any Client Property which Accenture accesses to perform the Services and that Client is authorized to instruct Accenture to perform the Services on or using such Client Property. For the avoidance of doubt, this Section will survive termination or expiration of this Agreement.

Client Property: means computer systems or automation and control systems; servers; technology infrastructures; telecommunications or electronic communications systems and associated communications; electronic systems for monitoring or controlling physical processes; Confidential Information; data (including Client's Personal Data); IP addresses, physical and/or intangible assets; equipment, devices; intellectual property; and/or physical premises, that are used by the Client, its employees, contractors, customers, or suppliers, whether owned or otherwise controlled by the Client or owned by a third party.

B) WARRANTIES

Notwithstanding anything in the Agreement to the contrary, the parties agree and acknowledge that: ACCENTURE DOES NOT REPRESENT, WARRANT, OR COVENANT THAT THE SERVICES PERFORMED UNDER THIS AGREEMENT WILL: (A) DETECT OR IDENTIFY ALL SECURITY OR NETWORK THREATS TO, OR VULNERABILITIES OF CLIENT'S NETWORKS OR OTHER FACILITIES, ASSETS, OR OPERATIONS; (B) PREVENT INTRUSIONS INTO OR ANY DAMAGE TO CLIENT'S NETWORKS OR OTHER FACILITIES, ASSETS, OR OPERATIONS; (C) RETURN CONTROL OF CLIENT OR THIRD PARTY SYSTEMS WHERE UNAUTHORIZED ACCESS OR CONTROL HAS OCCURRED; OR (D) MEET OR HELP CLIENT MEET ANY INDUSTRY STANDARD OR ANY OTHER REQUIREMENTS INCLUDING THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARD.

C) METADATA

Client authorizes Accenture to retain for its business purposes any indicators of compromise, malware, vulnerabilities, anomalies, or other metadata found as part of, or related to, the performance of the Services ("**Metadata**"). Accenture will de-identify such Metadata, and then may analyze, copy, store, and use such Metadata for purposes of improving security, including development of threat intelligence resources.

D) LIABILITY

In no event will either Party be liable (whether in contract, tort, negligence, strict liability in tort, by statute or otherwise) for any: (i) consequential, indirect, incident, special or punitive damages, or (ii) loss of profits, business, opportunity or anticipated savings, or loss or corruption of data (whether directly or indirectly arising). Accenture will not be liable for any loss arising out of any opinion or finding concerning the potential identity of any party responsible for a network compromise or data breach, or any decision by Client's insurer to reject or deny, in whole or in part, a claim by Client under its insurance policy. Nothing in this Agreement excludes or limits either Party's liability to the other which cannot lawfully be excluded or limited.

**Attachment A-1
(Standard Agreement)
Cyber Defense Supplement**

E) PERSONAL DATA

The Services may necessitate Accenture gaining access to (or obtaining incidentally) Client Personal Data. Notwithstanding anything in the Agreement to the contrary, this Section 5 (Personal Data) and the attached Exhibits I and II shall describe the Parties' responsibilities with respect to Personal Data. The types of Personal Data that may be processed by Accenture may include: personal contact information such as name, business address, business phone number, home address, home telephone or mobile number, fax number, email address, and passwords, user ids, information concerning family, lifestyle and social circumstances including age, date of birth, marital status, number of children and name(s) of spouse and/or children; employment details including employer name, job title and function, employment history, salary and other benefits, job performance and other capabilities, education/qualification, identification numbers, social security details; financial details including bank account data, credit or debit card data, payment or purchase history, device identifiers (such as serial numbers, mobile phone UDIDs), Internet Web Universal Resource Locators (URLS) and Internet Protocol (IP) addresses, video or audio images, or any other Personal Data contained within the systems with respect to which the Services are provided or reviewed in the course of the Services. The Personal Data may concern the following special categories of data: racial or ethnic origin; political opinions; religious or philosophical beliefs; trade union membership; data concerning health or sex life and sexual orientation; genetic data; and biometric data where processed to uniquely identify a person. The categories of data subjects involved may include any of Client's representatives, such as employees, job applicants, contractors, collaborators, partners, and customers of the Client.

**Attachment A-1, Exhibit I
(Standard Agreement)
Data Privacy and Security****DATA PRIVACY AND SECURITY**

This Exhibit describes the responsibilities of the parties with respect to the processing and security of any Client Personal Data in connection with the Services provided under this Agreement. Terms not defined below shall have the meaning set forth in the Agreement. In the event of a conflict between the Agreement and this Exhibit, this Exhibit shall prevail.

1. DEFINITIONS.

(a) "Business Contact Information" means the names, mailing addresses, email addresses, and phone numbers regarding the other party employees, directors, vendors, agents and customers, maintained by a party for its own business purposes as further described in Section 9 below.

(b) "Client Personal Data" means client-owned or controlled personal data provided by or on behalf of Client to Accenture or an Accenture affiliate or subcontractor for processing under this Agreement.

(c) "Data Protection Laws" means all applicable data protection and privacy Laws that apply to the processing of personal data under this Agreement, including, as applicable, the European Data Protection Laws.

(d) "European Data Protection Laws" means (i) the EU General Data Protection Regulation 2016/679 ("GDPR"), (ii) the Federal Data Protection Act of 19 June 1992 (Switzerland), and (iii) the UK Data Protection Law post-Brexit, and any US state or federal Laws or regulations pertaining to the collection, use, disclosure, security or protection of personal data, or to security breach notification, e.g., the California Consumer Privacy Act of 2018 ("CCPA").

(e) "Information Security Incident" means a breach of Accenture's security leading to the accidental or unlawful destruction, loss, alteration or unauthorized acquisition, disclosure, misuse or access to unencrypted Client Personal Data transmitted, stored or otherwise processed by Accenture.

(f) "Subprocessors" means third parties authorized under the terms of this Exhibit to have access to and process Client Personal Data in order to provide a portion of the Services.

(g) The terms "controller," "data subject," "personal data," "process," "processing," "processor" and "supervisory authority" as used in this Exhibit have the meanings given in the applicable Data Protection Laws, as relevant.

2. ROLES OF THE PARTIES; COMPLIANCE WITH DATA PROTECTION LAWS.

(a) Each party will comply with the requirements of the Data Protection Laws as applicable to such party with respect to the processing of the Client Personal Data.

(b) Client warrants to Accenture that it has all necessary rights to provide the Client Personal Data to Accenture for the processing to be performed in relation to the Services.

(c) Accenture will process the Client Personal Data only in accordance with Client's documented processing instructions as set forth in this Agreement, including this Exhibit, unless otherwise required by law.

(d) If Accenture is acting as a subcontractor to Client, Client warrants to Accenture that Client's instructions with respect to the Client Personal Data have been authorized by the applicable data owner/controller, including the appointment of Accenture as another processor.

(e) Except as otherwise set forth in the Agreement, (i) Accenture is a service provider and/or processor with respect to the Client Personal Data; and (ii) Client is an owner and/or controller or processor, as applicable, of the Client Personal Data.

(f) The Agreement shall set out (i) the subject matter and duration of the processing; (ii) the nature and purpose of the processing; and (iii) the type of personal data (e.g. sensitive, emails, health data) and categories of data subjects (e.g. employees, consumers, customers) involved.

3. DISCLOSURE AND USE OF DATA.

(a) Accenture shall not:

(i) sell any Client Personal Data;

(ii) retain, use or disclose any Client Personal Data for any purpose other than fulfilling its obligations and performing services in accordance with the Agreement; or

(iii) retain, use or disclose the Client Personal Data outside the direct business relationship between Accenture and Client, as set forth in the Agreement, including this Exhibit, unless otherwise required by law.

(b) Following expiration or termination of the Agreement or at Client's request, Accenture shall (and require that its sub-processors) promptly and securely delete (or return to Client) all Client Personal Data (including existing copies), unless otherwise required or permitted by applicable laws. Unless otherwise agreed, Accenture will comply with any Client deletion instruction as soon as reasonably practicable and within a maximum period of 180 days.

(c) Client agrees that execution of the Agreement by Accenture shall be deemed to constitute any certification that is required under applicable Data Protection Law to the restrictions on sale, retention, use, or disclosure of Client Personal Data herein.

(d) Notwithstanding subsection (b) above, in the course of providing the Services, Accenture may anonymize, aggregate, and/or otherwise de-identify Client data ("De-Identified Data") and subsequently use and/or disclose such De-Identified Data for the purpose of research, benchmarking, improving Accenture's Security offerings generally, or developing threat intelligence resources aimed at improving security generally; provided that Accenture has implemented technical safeguards and business processes designed to prevent the re-identification or inadvertent release of the De-Identified Data.

4. SECURITY OBLIGATIONS.

(a) Each party shall implement appropriate technical, physical and organizational security measures to safeguard Client Personal Data from unauthorized processing or accidental loss or damage, as further described below and the Agreement. Accenture has implemented and will maintain such measures, internal controls and information security routines intended to protect Client Personal Data in Accenture environments against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction ("Data Safeguards"), a more detailed description of which is described in Exhibit II.

**Attachment A-1, Exhibit I
(Standard Agreement)
Data Privacy and Security**

(b) Taking into account the ongoing state of technological development, the costs of implementation and the nature, scope, context and purposes of the processing of the Client Personal Data, as well as the likelihood and severity of risk to individuals, Accenture's implementation of and compliance with the security measures set forth in the Data Safeguards provide a level of security appropriate to the risk in respect of the processing of the Client Personal Data.

(c) Client and Accenture will each maintain and comply with globally applicable policies, standards and procedures intended to protect data within their own respective environments (e.g., systems, networks, facilities) and such policies will govern and control in their respective environments. For clarity, each Party will comply with the other Party's policies when accessing or operating within the other party's environments; provided that, The Parties acknowledge and agree that to the extent the Services involve circumvention of such policies, a breach of the policies arising from good faith performance of the Services will not be considered a breach of the Data Safeguards or this Agreement.

5. ADDITIONAL ACCENTURE RESPONSIBILITIES.

(a) Documentation, Audits and Inspections. Accenture shall make available to Client information reasonably requested by Client to demonstrate Accenture's compliance with its obligations in this Section and submit to audits and inspections by Client (or Client directed third parties) in accordance with a mutually agreed process designed to avoid disruption of the Services and protect the confidential information of Accenture and its other clients. As required by applicable law, Accenture shall inform Client if, in Accenture's opinion, any Client audit instruction infringes upon any applicable Data Protection Law. Client shall be solely responsible for determining whether the Services and Accenture's security measures as set forth in the Data Safeguards and the Agreement will meet Client's needs, including with respect to any Data Protection Laws.

(b) Data Subject and Supervisory Authority Requests. As required by law, and taking into account the nature of the Services provided, Accenture shall:

(i) provide assistance to Client as reasonably requested with respect to Client's obligations to respond to requests from Client's data subjects as required under applicable Data Protection Laws. Accenture will not independently respond to such requests from Client's data subjects, but will refer them to Client, except where required by applicable Data Protection Law; and

(ii) provide assistance to Client as reasonably requested if Client needs to provide information (including details of the Services provided by Accenture) to a competent supervisory authority, to the extent that such information is solely in the possession of Accenture or its Subprocessors.

(c) Privacy / Data Protection Impact Assessments. As required by law, and taking into account the nature of the Services provided and the information available to Accenture, Accenture shall provide assistance to Client as reasonably requested with respect to Client's obligations to conduct privacy / data protection impact assessments with respect to the processing of Client Personal Data as required under applicable Data Protection Laws.

6. **SUBPROCESSORS.** Client specifically authorizes the engagement of Accenture's affiliates as Subprocessors and generally authorizes the engagement of other third parties as Subprocessors as identified in the applicable Agreement. Accenture shall contractually require any such subprocessors to comply with data protection obligations that are at least as restrictive as those Accenture is required to comply with hereunder. Accenture shall remain fully liable for the performance of the Subprocessor. Accenture shall provide Client with written notice of any intended changes to the authorized Subprocessors and Client shall promptly, and in any event within 10 business days, notify Accenture in writing of any reasonable objection to such changes. If Client's objection is based on anything other than the proposed subprocessor's inability to comply with agreed data protection obligations, then any further adjustments shall be at Client's cost. Any disagreements between the parties shall be resolved via the contract dispute resolution procedure.

7. **CROSS-BORDER TRANSFERS OF CLIENT PERSONAL DATA.** Reserved.

8. **INFORMATION SECURITY INCIDENTS.** Accenture shall maintain procedures to detect and respond to Information Security Incidents. If an Information Security Incident occurs which may reasonably compromise the security or privacy of Client Personal Data, Accenture will promptly notify Client without undue delay. Accenture will cooperate with Client in investigating the Information Security Incident and, taking into account the nature of the Services provided and the information available to Accenture, provide assistance to Client as reasonably requested with respect to Client's breach notification obligations under any applicable Data Protection Laws.

9. **USE OF BUSINESS CONTACT INFORMATION.** Each party consents to the other party using its Business Contact Information for contract management, payment processing, service offering, and business development purposes related to the Agreement and such other purposes as set out in the using party's global data privacy policy (copies of which shall be made available upon request). For such purposes, and notwithstanding anything else set forth in this Agreement with respect to Client Personal Data in general, each party shall be considered a data controller with respect to the other party's Business Contact Information and shall be entitled to transfer such information to any country where such party's global organization operate

**Attachment A-1, Exhibit II
(Standard Agreement)
Data Safeguards for Client Data**

DATA SAFEGAURDS FOR CLIENT DATA

These data safeguards ("**Data Safeguards**") set forth the security framework that Client and Accenture will follow with respect to protecting data of Client ("**Client Data**") in connection with the Agreement in place between the Parties. In the event of a conflict between these Data Safeguards and any terms and conditions set forth in the Agreement, the terms and conditions of these Data Safeguards shall prevail.

- I. **Controlling Standards.** Each Party will maintain and comply with globally applicable policies, standards and procedures intended to protect data within their own respective environments (e.g., systems, networks, facilities) and such policies will govern and control in their respective environments. For clarity, each Party will comply with the other Party's policies when accessing or operating within the other Party's environments. Each Party will provide timely notice of any changes to such policies that may materially degrade the security of the Services, after which the Parties will equitably adjust the terms of the applicable SOW as necessary to appropriately address risk. Each Party will not use software or hardware that is past its End of Life (EOL) in connection with the Services without a mutually agreed risk management process for such items.
- II. **Vulnerabilities in Client Systems.** Unless otherwise expressly agreed in the applicable SOW, and except with respect to vulnerabilities caused by Accenture's breach of its obligations under the Agreement or applicable SOW, Client is responsible to remediate any vulnerabilities in Client Data or Client Systems at Client's cost. Client may engage Accenture to perform such remediation on Client's behalf pursuant to a Project SOW. For clarity, such remediation activities pursuant to a Project SOW are not considered "Services" under any other SOW. In the event Client fails to remediate a security vulnerability in Client Data or Client Systems, Accenture will not be liable for the consequences resulting from such security vulnerability, including a data security breach, except to the extent such security vulnerability resulted from Accenture's breach of its obligations under the Agreement or applicable SOW.
- III. **Penetration Testing of Accenture Systems.**
 1. Accenture will perform annual penetration tests on Accenture's IT environments in accordance with Accenture's internal security policies and standard practices.
 2. Accenture agrees to share with Client summary level information related to such tests as conducted by Accenture to the extent applicable to the Services.
 3. For clarity, as it relates to such penetration testing, Client will not be entitled to (i) data or information of other customers or clients of Accenture; (ii) test third party IT environments except to the extent Accenture has the right to allow such testing; (iii) any access to or testing of shared service infrastructure or environments, or (iv) any other Confidential Information of Accenture that is not directly relevant to such tests and the Services.
 4. For any Accenture IT systems that are physically dedicated to Client, the Parties may agree to separate, written testing plans.

**Attachment A-1, Exhibit II
(Standard Agreement)
Data Safeguards for Client Data**

- IV. Remote Work.** Accenture personnel may perform the Services or any portion of the Services remotely, provided that performing remotely does not (i) adversely impact Accenture's ability to perform its obligations under the Agreement; or (ii) require any increase to the fees.

For Services provided on a remote basis, any contractual requirements to provide physical and environmental security controls (e.g., secure bays; security guards; CCTV) at the Accenture service locations will not apply to remote work locations. In addition, where Accenture personnel are required to access Client systems from a remote work location, such access will only occur using devices and access points approved by Client.

- V. Technical and Organizational Measures.** Without limiting the generality of the foregoing and subject to any other express agreement between the Parties with respect to the Services as set forth in the applicable description of Services ("SOW"), the Parties have implemented and will maintain appropriate technical and organizational measures, internal controls, and information security routines intended to protect Client Data in their respective environments against accidental, unauthorized or unlawful access, disclosure, alteration, loss, or destruction, as set out below. To the extent the Client Data includes Personal Data, the implementation of and compliance with these measures and any additional security measures set out in the SOW are designed to provide an appropriate level of security in respect of the processing of the Client Personal Data.

1. Organization of Information Security

- a) Security Ownership.** Each Party will appoint one or more security officers responsible for coordinating and monitoring the security rules and procedures.
- b) Security Roles and Responsibilities.** Each Party's personnel with access to Client Data will be subject to confidentiality obligations.
- c) Risk Management Program.** Each Party will have a risk management program in place to identify, assess and take appropriate actions with respect to risks related to the processing of the Client Data in connection with the applicable Agreement between the Parties.

2. Asset Management

- a) Asset Inventory.** Each Party will maintain a complete asset inventory of its infrastructure, network, applications and cloud environments. Each Party will also maintain an inventory of all of its media on which Client Data is stored. Access to the inventories of such media will be restricted to that Parties' personnel authorized in writing to have such access.
- b) Data Handling.** Each Party will
 - i. Classify Client Data to help identify such data and to allow for access to it to be appropriately restricted.
 - ii. Limit printing of Client Data from its systems to what is minimally necessary to perform services and have procedures for disposing of printed materials that contain Client Data.
 - iii. Require its personnel to obtain appropriate authorization prior to storing Client Data outside of contractually approved locations and systems, remotely accessing Client Data, or processing Client Data outside the Parties' facilities.

**Attachment A-1, Exhibit II
(Standard Agreement)
Data Safeguards for Client Data**

3. Human Resources Security

- a) Security Training.** Each Party will
 - i. Inform its personnel about relevant security procedures and their respective roles.
 - ii. Inform its personnel of possible consequences of breaching the security rules and procedures.
 - iii. Only use anonymous data in training.

4. Physical and Environmental Security

- a) Physical Access to Facilities.** Each Party will only allow authorized individuals to access its facilities where information systems that process Client Data are located.
- b) Physical Access to Components.** Each Party will maintain records of the incoming and outgoing media containing Client Data, including the kind of media, the authorized sender/recipients, date and time, the number of media, and the types of Client Data they contain.
- c) Component Disposal.** Each Party will use industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) processes to delete Client Data when it is no longer needed.

5. Communications and Operations Management

- a) Operational Policy.** Each Party will maintain security documents describing its security measures and the relevant procedures and responsibilities of its personnel who have access to Client Data.
- b) Mobile Device Management (MDM)/Mobile Application Management (MAM).** Each Party will maintain a policy for its mobile devices that:
 - i. Enforces device encryption.
 - ii. Prohibit use of blacklisted apps.
 - iii. Prohibits enrollment of mobile devices that have been "jail broken."
- c) Data Recovery Procedures.** Each Party will
 - i. Have specific data recovery procedures with respect to its systems, in place designed to enable the recovery of Client Data being maintained in its systems.
 - ii. Review its data recovery procedures at least annually.
 - iii. Log data restoration efforts with respect to its systems, including the person responsible, the description of the restored data and where applicable, the person responsible and which data (if any) had to be input manually in the data recovery process.
- d) Malicious Software.** Each Party will have anti-malware controls to help avoid malicious software gaining unauthorized access to Client Data, including malicious software originating from public networks.

**Attachment A-1, Exhibit II
(Standard Agreement)
Data Safeguards for Client Data**

e) Data Beyond Boundaries. Each Party will

- i. Encrypt Client Data that it transmits over public networks.
- ii. Protect Client Data in media leaving its facilities (e.g., through encryption).
- iii. Implement automated tools where practicable to reduce the risks of misdirected email, letters, and / or faxes from its systems.

f) Event Logging.

- i. For its systems containing Client Data, each Party will log events consistent with its stated policies or standards.

6. Access Control

a) Access Policy. Each Party will maintain a record of security privileges of individuals having access to Client Data via its systems.

b) Access Authorization. Each Party will

- i. Maintain and update a record of personnel authorized to access Client Data via its systems.
- ii. When responsible for access provisioning, promptly provision authentication credentials.
- iii. Deactivate authentication credentials where such credentials have not been used for a period of time (such period of non-use not to exceed 90 days).
- iv. Deactivate authentication credentials upon notification that access is no longer needed (e.g. employee termination, project reassignment, etc.) within two business days.
- v. Identify those personnel who may grant, alter or cancel authorized access to data and resources.
- vi. Ensure that where more than one individual has access to its systems containing Client Data, the individuals have unique identifiers/log-ins (i.e., no shared ids).

c) Least Privilege. Each Party will

- i. Only permit its technical support personnel to have access to Client Data when needed
- ii. Maintain controls that enable emergency access to productions systems via firefighter ids, temporary ids or ids managed by a Privileged Access Management (PAM) solution.
- iii. Restrict access to Client Data in its systems to only those individuals who require such access to perform their job function.
- iv. Limit access to Client Data in its systems to only that data minimally necessary to perform the services.
- v. Support segregation of duties between its environments so that no individual person has access to perform tasks that create a security conflict of interest (e.g., developer/reviewer, developer/tester).

**Attachment A-1, Exhibit II
(Standard Agreement)
Data Safeguards for Client Data**

- d) **Client Data in Non-Production Systems.** Client agrees to provide masked or fictitious Client Data for use in non-production systems.
 - e) **Integrity and Confidentiality.** Each Party will instruct its personnel to disable administrative sessions when leaving premises or when computers are otherwise left unattended.
 - f) **Authentication.** Each Party will
 - i. Use industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) practices to identify and authenticate users who attempt to access its information systems.
 - ii. Where authentication mechanisms are based on passwords, require that the passwords are renewed regularly.
 - iii. Where authentication mechanisms are based on passwords, require the password to contain at least eight characters and three of the following four types of characters: numeric (0-9), lowercase (a-z), uppercase (A-Z), special (e.g., !, *, &, etc.).
 - iv. Ensure that de-activated or expired identifiers are not granted to other individuals.
 - v. Monitor repeated attempts to gain access to its information systems using an invalid password.
 - vi. Maintain industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) procedures to deactivate passwords that have been corrupted or inadvertently disclosed.
 - vii. Use industry standard (e.g., ISO 27001, CIS Sans 20, and/or NIST Cyber-Security Framework, as applicable) password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, as well as during storage.
 - g) **Multi Factor Authentication.** Each Party will implement Multi-Factor Authentication for internal access and remote access over virtual private network (VPN) to its systems.
7. **Network and Application Design and Management.** Each Party will
- a) Have controls to avoid individuals gaining unauthorized access to Client Data in its systems.
 - b) Use email-based data loss prevention to monitor or restrict movement of sensitive data.
 - c) Use network-based web filtering to prevent access to unauthorized sites.
 - d) Use firefighter IDs or temporary user IDs for production access.
 - e) Use network intrusion detection and / or prevention in its systems.
 - f) Use secure coding standards.
 - g) Scan for and remediate OWASP vulnerabilities in its systems.
 - h) To the extent technically possible, work together to limit the ability of Accenture personnel to access non-Client and non-Accenture environments from the Client systems.

**Attachment A-1, Exhibit II
(Standard Agreement)
Data Safeguards for Client Data**

- i) Maintain up to date server, network, infrastructure, application and cloud security configuration standards.
- j) Scan their respective environments to ensure identified configuration vulnerabilities have been remediated.

8. Patch Management

- a) Each Party will have a patch management procedure that deploys security patches for its systems used to process Client Data that includes:
 - i. Defined time allowed to implement patches (not to exceed 90 days for high or medium patches as defined by the Party's respective standard); and
 - ii. Established process to handle emergency or critical patches as soon as practicable.

9. Workstations

- a) Each Party will implement controls for all workstations it provides that are used in connection with service delivery/receipt incorporating the following:
 - a. Software agent that manages overall compliance of workstation and reports at a minimum on a weekly basis to a central server
 - b. Encrypted hard drive
 - c. Patching process so that workstations are patched within the documented patching schedule
 - d. Ability to prevent blacklisted software from being installed
 - e. Antivirus with a minimum weekly scan
 - f. Firewalls installed

10. Information Security Breach Management

- a) **Security Breach Response Process.** Each Party will maintain a record of its own security breaches in its systems with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the process for recovering data.
- b) **Service Monitoring.** Each Party's security personnel will review their own logs as part of their security breach response process to propose remediation efforts if necessary.

11. Business Continuity Management

- a) Each Party will have processes and programs that are aligned to ISO 22301 to enable recovery from events that impact its ability to perform in accordance with the Agreement.

**Attachment A-2
(Standard Agreement)
Remote Work Protocols**

REMOTE WORK PROTOCOLS

This Attachment sets out the remote work protocols to be followed by the Parties.

Workstations: Accenture will implement controls for all workstations/laptops on Accenture provided devices that are used in connection with service delivery/receipt incorporating the following:

- Software agent that manages overall compliance of workstation and reports a minimum monthly to a central server;
- Encrypted hard drive;
- Patching process to ensure workstations are current on all required patches;
- Ability to prevent non-approved software from being installed (e.g., peer-to-peer software);
- Antivirus with a minimum weekly scan;
- Firewalls installed;
- Data Loss Prevention tool (subject to any legal requirements, e.g. Works Council); and
- Web filtering.

Access Control:

- Two factors authentications are enabled on Client and Accenture VPN;
- Client will promptly provision authentication credentials, including any additional requirements to support Client's two factor authentication;
- Client and Accenture will promptly deactivate authentication credentials where such credentials have not been used for a period of time (such period of non-use not to exceed six months);
- Client and Accenture will deactivate authentication credentials upon notification that access is no longer needed (e.g. employee termination, project reassignment, etc.) within two business days; and
- Client and Accenture to manage the access controls using the least privilege access protocols where applicable.

Connectivity:

- Where Accenture personnel connect to Accenture networks and infrastructure, Accenture is responsible for applying Accenture standard technical and organizational security controls to such Accenture-provided workstation/laptop and the Accenture environment.

**Attachment A-2
(Standard Agreement)
Remote Work Protocols**

- Where Accenture personnel are using Accenture or Client provided desktop and/or laptops and accessing the Client network, environments and systems, via VDI, Client is responsible for applying Client's standard technical and organizational security controls in respect of such network, environments and systems to the Client's network and environments.
- Accenture cannot confirm that the wireless network used by such Accenture personnel is protected with agreed upon security standards.

Physical Controls: Any contractual requirements to provide specific physical and environmental security controls at the Accenture personnel's work location when working remotely will not apply, including, but not limited to, the following:

- Secure bays;
- Presence of security guards to prevent unauthorized resources from accessing the work site;
- Use of CCTV to monitor access and the work environment;
- Use of cross-cut shredders to dispose of hard copy;
- Prohibition of cell phones and other cameras during work.

Client Standards: To the extent reasonably possible, Accenture personnel working remotely will continue to abide by the applicable Client policies and standards in performing the Services. Such policies govern and control within the Client's systems and environments.

**Attachment A-3
(Standard Agreement)
AIP+ Addendum**

AIP+ ADDENDUM

AIP+ POC AGREEMENT – NO CLIENT ACCESS (U.S.)

ORDER FORM (EXHIBIT A)

Term of Agreement ("Term"): 365 days from the Effective Date.

Description of Proof of Concept ("POC"): Provision an AIP+ environment to support California Employment Development Department's fraud data analytics and reporting requirements.

Platform and Applications:

- ☒ Applied Intelligence Platform+ (AIP+)
- ☒ AIP+ Applications
 - Tableau Creator
 - Tableau Viewer
 - Microsoft R Open
 - Python

Development Environment:

The Platform will be provisioned with the following configuration.

Product Name	OS Type (Redhat, Linux, Windows)	Server/Service configuration	# of resources	EBS Volume (OS)	Storage/ EBS Volume (Data)
AWS Postgres RDS	NA	db.m5.2xlarge	NA	NA	2 TB
AWS S3	NA	NA	NA	NA	2 TB
Tableau Creator + Viewer	MSWIN	r5.2xlarge	1	160 GB	640 GB
Microsoft R Open + Python	RHEL	r5.2xlarge	1	160 GB	640 GB
AWS Glue ETL	NA	5 DPU's, 200 hours per month	NA	NA	NA
AWS KMS – Free Tier	NA	NA	NA	NA	NA
FortiWeb Marketplace	Linux	c5.large	1	32 GB	NA
FortiGate Marketplace	Linux	c5.large	1	160 GB	NA
Vormetric Data Security Manager	RHEL	c5.large	1	160 GB	90GB
Kubernetes Master (Nagios Core/Proftpd/ELK/Symantec)	Linux	c5.xlarge	1	160 GB	200GB
Active Directory/ Remote Desktop	MSWIN	m5.large	1	160 GB	NA
Jump Host	MSWIN	m5.xlarge	1	160 GB	NA

Client Responsibilities: None

Fees: \$0.00

Assumptions for Client's Platform audit requirements:

- Client will identify a maximum of 3 users for Platform access
- Client users will be provided the following access to the Platform –
 - Connect to the Jump Host via Virtual Private Network (FortiClient)

**Attachment A-3
(Standard Agreement)
AIP+ Addendum**

- Access AWS S3 buckets and AWS Postgres database to view the data
- AIP+ will provide a quarterly report with list of users who have access to the platform

Description of Client Content: sensitive personally identifiable information (PII) and financial data in scope; employee and claims data

Data Volume Limit: < 2 TB of data in total

Data Upload limit: < 5 GB per day

Number of Users:

Software	# of users
MS Open R + Python	5
Tableau Creator	2
Tableau Viewer	25
Remote Desktop	7

Territory: US West (N. California)

This Order Form, Exhibit A (Terms and Conditions), and the following selected Exhibits, which Exhibits are attached hereto, constitute the entire agreement ("Agreement") between Accenture LLP (inclusive of its Affiliates, "Accenture") and the entity that appears below as "Client" and govern Client's access to and use of the Platform during the POC:

- ☒ Exhibit B Cloud Services Vendor Terms
- ☒ Exhibit C Data Processing and Security Terms

IN WITNESS WHEREOF, the parties hereby execute this Agreement by their duly authorized representatives, effective as of the date signed by the last party (the "Effective Date").

Accenture:

California Employment Development Department (Client)

By: _____

By: _____

Printed name: _____

Printed name: _____

Title: _____

Title: _____

Date: _____

Date: _____

**Attachment A-3, Exhibit A
(Standard Agreement)
Terms and Conditions**

1. **Use and Access.** Accenture grants Client the right to access via the Internet and use the Platform during the Term for Client's internal evaluation purposes in the Territory. The POC will use the Platform, hosted in the cloud by Accenture's Cloud Service Vendor (CSV). Client may also receive access to Outputs.

2. **Client Content.** Reasonable and appropriate measures will be implemented that are designed to secure Client Content within Accenture's or CSV's control against loss or unauthorized access or disclosure. The Platform is subject to the CSV's Acceptable Use and Service Terms Policies, each as modified by the CSV from time to time (Policies), links to the current versions of which are included in Exhibit B. Client has collected and shall maintain and handle all Client Personal Information contained in Client Content in compliance with all applicable data privacy and protection laws, rules and regulations. Client authorizes Accenture to process Client Personal Information in accordance with the Data Processing and Security Terms attached to this Agreement in Exhibit C. Client warrants that Client provides Client Content that complies with all applicable laws and that such Client Content does not infringe the intellectual property rights of any third party. Client warrants that it has provided all required notices, has a lawful basis and/or obtained all required consents and/or authorizations, and registrations to disclose and transfer any Client Personal Information to Accenture and for the use of such Client Personal Data in manner contemplated by this Agreement and the relevant Order Form. Client will promptly notify Accenture of any failure to comply with this requirement and will defend, indemnify, and hold harmless Accenture and its Affiliates from and against any Losses relating to any claim arising out of such failure. Client shall use industry standard methods and tools to prevent introduction to the Platform of any viruses, malicious files or other harmful code or any other similar software that may access or damage the operation of the Platform. Accenture's licensors are third party beneficiaries under this Agreement for enforcement purposes. Client is solely responsible for backing up the Client Content unless otherwise agreed in writing. Client grants to Accenture a non-exclusive license to use, import, host, store, process, modify and transfer the Client Content into the Platform (as a batch or in real time) for purposes of this POC. Incidental data may include, but not be limited to, use usage patterns, trends, statistics, and other data derived from use of the Platform (but not Client Content itself) for purposes of supporting, developing or improving the Platform and other Accenture products and services. Upon expiration or termination of the Agreement, Accenture agrees to destroy any Client Content in accordance with this Agreement.

3. **Ownership.** As between Client and Accenture: (i) Accenture owns all intellectual property rights in the Output and the Platform and any suggestions, ideas, enhancement requests, feedback, recommendations or other information provided by Client relating to the Platform; and (ii) Client owns all Client Content.

4. **Restrictions.** Client will not, and will ensure that its Users will not, directly or indirectly: (i) access or use the Platform to host or transmit any content, data or information that is illegal or which infringes any third party's rights, such as intellectual property rights or right of privacy, or which otherwise violates any applicable laws; (ii) copy, translate, make derivative works, disassemble, decompile, reverse engineer or otherwise attempt to discover the source code or underlying ideas or algorithms embodied in the software applications or other systems used for the

provision of the Platform (including the Infrastructure Services), unless expressly permitted under any applicable laws, or remove any titles or trademarks, copyrights or restricted rights notices in the systems, software and other materials used in the provision of the Platform; (iii) use any such software application either to access a database outside of the Platform or to develop a product that is competitive with such software application; (iv) make any benchmarking results for any such software application available to any third parties; (v) Access or use the Platform for the purpose of building products or services that compete with the Platform, whether by copying its features or user interface; (vi) interfere with or disrupt the Platform, the data contained in the Platform or the networks connected to the Platform; or (vii) use, or permit the use of, the Platform in a live or production environment or in any manner except as specifically set forth herein. Client is responsible for use of the Platform by any User. Client will notify Accenture promptly upon becoming aware of any possible misuse of its accounts or any security incident related to the Platform. Accenture reserves the right to introduce commercially reasonable changes to the Platform from time to time and to suspend, block and/or otherwise limit Client's access to or use of the Platform without notice if Accenture determines, in its sole discretion, that the Platform or Accenture's network: (a) is being unreasonably burdened; (b) is being used in a way prohibited by law, regulation or governmental order or that could harm the Platform or the CSV's service or impair anyone else's use of either; (c) is being used to violate rights of others, to try to gain unauthorized access to or disrupt any service, device, data, account or network, to spam or distribute malware or for any other malicious use; (d) is being used in any application or situation where failure of the Platform could lead to the death or serious bodily injury of any person, or to severe physical or environmental damage; or (e) there is an actual or alleged security breach with respect to the Platform.

5. **Fees.** Client agrees to pay the fees specified in the Order Form ("Fees"). Billable expenses will be billed at actuals or capped as specified in the Order Form. Fees exclude applicable duties, tariffs, and taxes. All invoices submitted to Client for payment will be itemized in reasonable detail. Unless otherwise specified in the Order Form, fees will be due and payable within forty-five (45) days of Accenture's invoice. Late payments that are not the subject of a good faith dispute are subject to an interest charge, which is the lesser of: (i) one and one-half percent (1.5%) per month; or (ii) the maximum legal rate. Any taxes arising out of this Agreement other than those on Accenture's net income will be Client's responsibility. Accenture will pay any taxes remitted to it by Client to the applicable taxing authority when due.

6. **Confidentiality.** During the Term, each party may be given access to the Confidential Information of the other. Each party will protect the confidentiality of the other party's Confidential Information in the same manner that it protects the confidentiality of its own similar information, but in no event using less than a reasonable standard of care. Each party will restrict access to Confidential Information of the other party to those of its and its Affiliates' employees, contractors, licensors and agents with a need to know it for purposes of this Agreement ("Representatives"), provided that such recipients are bound by obligations of confidentiality substantially similar to the terms of this Agreement. Each party is responsible for its Representative's access to and use of Confidential Information. Nothing in this Agreement will prohibit or limit a party's use of information (including, but not limited to, ideas, concepts, know-how, techniques, and methodologies): (i) previously known to it without an obligation not to disclose such information; (ii) independently developed

**Attachment A-3, Exhibit A
(Standard Agreement)
Terms and Conditions**

by or for it without use of the information; (iii) acquired by it from a third party which was not lawfully under an obligation not to disclose such information; or (iv) which is or becomes publicly available through no breach of this Agreement. Each party will return or destroy the other party's Confidential Information in its possession upon request by the other party, provided that each party may retain copies of the other party's Confidential Information as required for compliance with its recordkeeping or quality assurance requirements. If the recipient receives a subpoena or other validly issued administrative or judicial process requesting Confidential Information of the other party, it will promptly notify the other party of such receipt. Unless the subpoena or process is timely limited, quashed or extended, the recipient will then be entitled to comply with such request to the extent permitted by law.

7. Compliance. Client will comply with all laws applicable to Client's business and Client's use of the Platform. Each party will comply with all export control and economic sanctions laws (together, the "Trade Control Laws") applicable to its performance under this Agreement. Client will not use the Platform in relation to any activities involving a country subject to comprehensive economic sanctions (including without limitation Cuba, Iran, North Korea, Sudan, Syria or Crimea), or involving a party in violation of applicable Trade Control Laws, or that require government authorization, without first obtaining the informed consent of Accenture and the required authorization. The Platform and Outputs are not intended to be used: (i) to prevent, diagnose or treat health or medical conditions; (ii) to monitor health or medical conditions for purposes of prevention or treatment of health or medical conditions; or (iii) as a medical device, medical application or medical monitoring platform. Further, the Platform and Outputs have not been evaluated by the Food and Drug Administration or similar regulatory agency for safety or effectiveness. Client shall be responsible to ensure that any services or products Client offers or sells in reliance on the Platform or Outputs are sold, marketed and distributed in compliance with all applicable Laws, including FDA, FTC and ONC regulations.

8. Disclaimer. THE OUTPUTS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, WHETHER EXPRESS, IMPLIED OR STATUTORY. ACCENTURE, ITS AFFILIATES AND ITS LICENSORS MAKE NO REPRESENTATIONS AND PROVIDE NO WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, REGARDING THE OUTPUTS. ACCENTURE, ITS AFFILIATES AND ITS LICENSORS EXPRESSLY DISCLAIM ALL WARRANTIES, EXPRESS, IMPLIED, STATUTORY OR OTHERWISE, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT, ANY WARRANTIES ARISING OUT OF ANY COURSE OF DEALING OR USAGE OF TRADE, AND ANY WARRANTIES OF FITNESS FOR HIGH RISK ACTIVITIES. THESE DISCLAIMERS SHALL ONLY APPLY TO THE EXTENT PERMITTED BY APPLICABLE LAW. Client acknowledges that Accenture does not control the transfer of data over the internet or any telecommunications network and shall not be responsible for any loss or corruption of Client Content during such transmission.

9. Limitations on Liability. Nothing in this Agreement will exclude or limit either party's liability: (i) for death or personal injury resulting from the negligence of either party or their agents or employees; (ii) for fraud or fraudulent misrepresentation; or (iii) for anything which cannot be

excluded or limited by law. Subject to the foregoing, NEITHER PARTY SHALL BE LIABLE TO THE OTHER UNDER OR IN CONNECTION WITH THIS AGREEMENT (WHETHER IN CONTRACT, TORT, INCLUDING, WITHOUT LIMITATION, NEGLIGENCE OR OTHERWISE) FOR ANY LOSS OF PROFIT, LOSS OF ANTICIPATED SAVINGS, LOSS OF BUSINESS OPPORTUNITY, LOSS OF OR CORRUPTION OF DATA, OR INDIRECT OR CONSEQUENTIAL LOSSES, IN EACH CASE SUFFERED OR INCURRED BY THE OTHER PARTY, WHETHER OR NOT SUCH LOSSES WERE WITHIN THE CONTEMPLATION OF THE PARTIES ON THE EFFECTIVE DATE OF THIS AGREEMENT. Subject to the above, and except for damages for breach of a party's indemnity obligations hereunder, each party's aggregate liability to the other arising from any given event or series of connected events under or in connection with this Agreement shall be limited to the amount paid or payable by Client under this Agreement; or, if the Order Form stipulates that the POC is provided at no charge to Client, USD \$1,000 or the equivalent in local currency.

10. Termination. Either Party may at any time and without cause terminate this Agreement upon thirty (30) days' prior written notice to the other party. Upon the expiration or earlier termination of this Agreement, Client's right to access and use the Platform will terminate and Client will, at Accenture's election, either return to Accenture or destroy any materials provided by Accenture related to the Platform. Client may keep and use downloaded Outputs. Client acknowledges that it may need to obtain the necessary licenses to the software required to view the Outputs.

11. Miscellaneous. The failure of a party to enforce a right will not constitute a waiver of the right. The provisions of this Agreement that are by their nature intended to do so shall survive the expiration or earlier termination of this Agreement. Neither party will use the other party's name or trademarks outside its organization without prior express written consent of the other party, which consent may be withheld in its sole discretion. Notwithstanding the foregoing, Accenture shall be permitted to refer to Client as a customer reference concerning the POC under this Agreement, for opportunities at existing and prospective Accenture clients. This Agreement, including the Order Form and any Exhibits, constitutes the entire agreement between the parties with respect to the Platform and may not be amended or modified other than in a writing signed by both parties. This Agreement shall be governed by and construed in accordance with the laws of the State of New York, without regard to its conflict of laws provisions.

12. Business Contact Information. Each party consents to the other party using its Business Contact Information for contract management, payment processing, service offering, and business development purposes related to this Agreement and such other purposes as set out in the using party's global data privacy policy (copies of which shall be made available upon request). For such purposes, and notwithstanding anything else set forth in this Agreement with respect to Client Personal Information in general, each party shall be considered a controller with respect to the other party's Business Contact Information and shall be entitled to transfer such information to any country where such party's global organization operates.

12. Definitions. In this Agreement:

Affiliate means any entity, whether incorporated or not, that is Controlled by, Controls, or is under common Control with Accenture, where **Control**

**Attachment A-3, Exhibit A
(Standard Agreement)
Terms and Conditions**

means the ability, whether directly or indirectly, to direct the affairs of another by means of ownership, contract or otherwise.

Client means the entity identified as such on the Order Form signature line.

Client Content means all content, data and materials that Client or Users enter into the Platform or are otherwise provided by or on behalf of Client for processing, analysis and/or display via the Platform.

Client Personal Information means Client-owned or controlled personal information (i.e. which names or identifies a natural person) provided to Accenture by or on behalf of Client in connection with this Agreement, in the form of Client Content. Unless prohibited by applicable Data Privacy Laws, Client Personal Information shall not include information or data that is anonymized, aggregated, de-identified and/or compiled on a generic basis and which does not name or identify a specific person.

Confidential Information means this Agreement and information that relates to the other party's past, present, or future research, development, business activities, products, services, and technical knowledge, which is identified by the discloser as confidential or that would be understood to be confidential by a reasonable person under the circumstances.

Consents means all necessary consents, permissions, notices and authorizations necessary for Accenture to provide the Platform, including any of the foregoing from Client employees or third parties; valid consents from or notices to applicable data subjects; and authorizations from regulatory authorities, employee representative bodies or other applicable third parties.

Data Privacy Laws means all applicable laws, regulations and regulatory guidance in relation to the processing or protection of Personal Information, as amended from time-to-time, including but not limited to, Regulation (EU) 2016/679 of 27 April 2016, General Data Protection Regulation ("GDPR").

Device means any end point of the system, including mobile phones, sensors, gateways, etc.

Losses means any claims, damages, losses, liabilities, costs and expenses (including reasonable legal fees).

Order Form means the order form signed by the parties and to which these terms and conditions are attached.

Outputs means downloadable files consisting of visualizations, charts, graphs, reports or other data displayed or produced via the Platform, but excluding software and Client Content.

Platform means the platform and applications identified on the Order Form, including without limitation the APIs, software services, models, algorithms, methodologies and approaches embodied in the foregoing, and any modifications and enhancements thereto. For purposes of clarification, the Platform does not include Client Content and any Client Confidential Information.

POC means the proof of concept described in the Order Form.

Term means the POC duration described in the Order Form.

Security Incident means a failure by Accenture to comply with the Security Standards, where such failure results in the unauthorized access to or acquisition of any unencrypted record in Accenture's control containing Client Content in a manner that renders misuse of the Client Content reasonably possible. For the avoidance of doubt, Security Incident does not include any of the following that results in no unauthorized access to Client Content or to any Accenture or Cloud Vendor systems storing Client Content: (a) pings and other broadcast attacks on firewalls or edge servers, (b) port scans, (c) unsuccessful log-on attempts, (d) denial of service attacks, (e) packet sniffing (or other unauthorized access to traffic data that does not result in access beyond IP addresses or headers), or (f) similar

incidents.

User means an individual or entity who, directly or indirectly through another User, has access to the Platform using Client's account (excluding any Accenture users).

**Attachment A-3, Exhibit B
(Standard Agreement)
Cloud Services Vendor Terms**

AWS Acceptable Use Policy as it may be updated from time to time: <http://aws.amazon.com/aup>

**Attachment A-3, Exhibit C
(Standard Agreement)
Data Processing and Security Terms**

These Data Processing and Security Terms apply to Client Personal Information processed by Accenture and its subprocessors on Client's behalf in connection with its provision/performance of the POC described in the related Order Form.

In the context of the POC, these Data Processing and Security Terms shall not apply to non-production environments if such environments are made available by Accenture (e.g. a test instance of the Platform), and Client shall not store Client Personal Information in such environments.

Client shall be the controller of Client Personal Information, and Accenture shall be the processor of such data and each Party shall comply with the relevant data privacy laws to the extent applicable to such Party in its respective role. Client warrants to Accenture that it has all necessary rights to provide the Client Personal Information to Accenture for the processing to be performed in relation to the Services. Client shall be responsible for obtaining all necessary consents, and providing all necessary notices, as required under the relevant Data Protection Laws in relation to the processing of the Client Personal Information.

The Parties hereby acknowledge and agree to the following with respect to the processing of any Client Personal Information under this Agreement:

1. Unless otherwise required by law, Accenture shall process Client Personal Information on Client's behalf as follows:
 - **The subject matter of the processing** is limited to the Client Personal Information identified in this document.
 - **The nature and purpose of the processing** shall be to provide the services as defined in the description of the POC in the relevant Order Form concluded between Client and Accenture.
 - **The duration of the processing** is the Term of the related Order Form.
 - **The types of Personal Information** include: name, phone numbers, date of birth, e-mail address, time zone, address data, system access / usage / authorization data, company name, contract data, wage data, invoice data.
 - **The categories of data subjects** are: unless provided otherwise by Client, will include employees, contractors, business partners or other individuals whose Personal Information is stored in the Platform.
2. Accenture will process Client Personal Information only in accordance with **Client's documented instructions**. These Data Processing and Security Terms constitute such documented initial instructions. Accenture shall use reasonable efforts to follow any other Client's instructions as long as they are required by law, technically feasible and do not require changes to the POC. If Client requires that Accenture follow a processing instruction that may generate additional costs for Accenture, a mutually agreed change request to the Agreement must be concluded in advance.

If Client requires that Accenture follow a processing instruction despite Accenture's notice that such instruction may, in Accenture's opinion, infringe an applicable Data Protection Law, Client shall be responsible for all liability, and shall defend, indemnify and hold Accenture harmless against all claims and damages, arising from any continued processing in accordance with such instruction.

3. All Accenture personnel, including subcontractors, authorized to process the Client Personal Information shall be subject to confidentiality obligations and/or subject to an appropriate statutory obligation of confidentiality.
4. When providing or making available Client Personal Information to Accenture, Client shall only disclose or transmit Client Personal Information that is necessary for Accenture to perform the services as set forth in this Agreement and the applicable Order Form. Accenture will process the Client Personal Information only in accordance with Client's documented processing instructions as set forth in this Agreement and the applicable Order Form, unless otherwise required by law. Accenture shall not:
 - a. sell any Client Personal Information;
 - b. retain, use or disclose any Client Personal Information for any purpose other than fulfilling its obligations and performing services in accordance with the Agreement; or
 - c. retain, use or disclose the Client Personal Information outside the direct business relationship between Accenture and Client, as set forth in the Agreement, including this Exhibit and the applicable Order Form, unless otherwise required by law.

**Attachment A-3, Exhibit C
(Standard Agreement)
Data Processing and Security Terms**

Client agrees that execution of the applicable Order Form by Accenture shall be deemed to constitute any certification required under applicable Data Privacy Laws to any restrictions on sale, retention, use, or disclosure of Client Personal Data herein. Notwithstanding subsections (1) – (3) above, Client agrees that in the course of providing the services, Accenture may host, store, use, process, modify, and transfer Client Personal Information for the purposes of the services as provided in this Agreement.

5. Each Party shall implement appropriate **technical and organizational security measures** to safeguard Client Personal Information from unauthorized processing or accidental loss or damage. Client acknowledges and agrees that, taking into account the ongoing state of technological development, the costs of implementation and the nature, scope, context and purposes of the processing of the Client Personal Information, as well as the likelihood and severity of risk to individuals, Accenture's implementation of and compliance with the security measures set forth in **Attachment A** to this document provide a level of security appropriate to the risk in respect of the processing of the Client Personal Information.
6. Client specifically authorizes the engagement of Accenture's affiliates as **subprocessors** and generally authorizes, for the POC, the engagement of Accenture's Cloud Vendor as subprocessor. Accenture shall contractually require any such subprocessors to comply with data protection obligations that are at least as restrictive as those Accenture is required to comply with hereunder to the extent applicable to the subprocessors' subcontracted services. Accenture shall remain fully liable for the performance of the subprocessors. Accenture shall provide Client with written notice of any intended changes to the authorized subprocessors and Client shall promptly, and in any event within 10 business days, notify Accenture in writing of any reasonable objection to such changes. If Client's objection is based on anything other than the proposed subprocessor's inability to comply with agreed data protection obligations, then any further adjustments shall be at Client's cost. The Parties will make their best efforts to settle on any disagreement that may occur.
7. As required by law and taking into account the nature of the processing, Accenture shall provide assistance to Client as reasonably requested in responding to requests by Client's data subjects as required under applicable Data Privacy Laws. Accenture will not independently respond to such requests, but will refer them to Client, except where required by applicable Data Privacy Laws.
8. Taking into account the nature of the processing and the information available to Accenture, when the processing is within the scope of the GDPR Accenture shall provide reasonable assistance to Client with respect to: (i) Client's implementation of appropriate security measures; (ii) Client's obligation to notify regulators and data subjects of a breach with respect to Client Personal Information as required by GDPR; (iii) Client's obligation to conduct data protection impact assessments with respect to the processing as required by GDPR; and (iv) Client's obligations to consult with regulators as required by GDPR. Client shall be responsible for the reasonable costs of such assistance.
9. Upon expiration or termination of the Services, Accenture **shall return or destroy** any Client Personal Information in accordance with the Client instruction as soon as reasonably practicable and within a maximum period of 180 days.
10. Accenture shall make available to Client information reasonably requested by Client to demonstrate Accenture's compliance with its obligations in these Data Processing and Security Terms and Accenture shall submit to **audits** and inspections by Client (or Client directed third parties) in accordance with a mutually agreed process designed to avoid disruption of the POC and protect the confidential information of Accenture, its authorized subprocessors and its other clients and in accordance with the following principles:
 - audit limited to once a year;
 - not to exceed 3 business days unless otherwise agreed by the parties in writing.
 - reasonable prior written notice (at least 60 days unless a data protection authority requires Client's earlier control under mandatory Data Protection Law).
 - scope and agenda of the audit to be determined in advance.

With regard to this section, Accenture shall inform Client if, in Accenture's opinion, any Client instruction infringes any applicable Data Privacy Law.

**Attachment A-3, Exhibit C
(Standard Agreement)
Data Processing and Security Terms**

In the context of the POC, Client acknowledges that Accenture's Cloud Vendor use external, independent auditors to audit and verify the adequacy of their security measures, including the security of their physical data centers, and generate an audit report, available annually ("Report"). The Reports are the Cloud Vendors' Confidential Information and will be available to Client, at Client's request, subject to Client executing the Cloud Vendor's standard non-disclosure agreement. Client agrees to exercise any right to conduct an audit or inspection of the Cloud Vendor, including under the EU Model Clauses (defined here below) if applicable, by instructing Accenture to obtain the relevant Cloud Vendor's Report, as described in this section. Client may change this instruction at any time upon written notice to Accenture, provided if the Cloud Vendor declines to submit to an audit or inspection requested by Client, Accenture will not be in breach of this Agreement, but Client is entitled to terminate the related Service Order to which such request relates upon 30 days' notice to Accenture. If the EU Model Clauses apply, nothing in this section modifies the EU Model Clauses, and nothing in this Section affects any supervisory authority's or data subject's rights under the EU Model Clauses.

11. As of the Effective Date of the relevant Order Form, **Client has identified for Accenture the countries where the data subjects originate.**
12. The Parties shall rely on the Standard Contractual Clauses for the Transfers of Personal Data to Processors Established in Third Countries, dated 5 February 2010 (2010/87/EU) as amended from time to time (the "EU Model Clauses") to protect Client Personal Information being transferred from a country within the European Economic Area to a country outside the European Union or Switzerland not recognized by the European Commission as providing an adequate level of protection for Personal Information. Where the transfer relies on the EU Model Clauses, the Client, acting as data exporter, shall execute, or shall procure that the relevant Client entities execute, such EU Model Clauses with the relevant Accenture entity or a third-party entity, acting as a data importer. On behalf of the Client and its affiliates as the data exporters, Client authorizes Accenture and/or its affiliates to execute EU Model Clauses with subprocessors located in countries without an adequacy finding by the EU Commission who will have access to Client Personal Information originating from the European Economic Area.

In the event that Client Personal Information is to be transferred from a country not within the European Economic Area to any other country in connection with the services described in this Agreement, where required by applicable data privacy law, the parties shall enter into a data transfer agreement to ensure the Client Personal Information is adequately protected. Client, acting as data exporter, shall execute, or shall procure that the relevant Client entities execute, such data transfer agreement, with the relevant Accenture entity or a third-party entity, acting as a data importer. If and when Accenture is authorized for Binding Corporate Rules for Processors, the parties shall rely on such Binding Corporate Rules for Processors to cover any cross-border transfer of Client Personal Information to Accenture, provided that Accenture (i) maintains and extends the applicable authorization of its Binding Corporate Rules for Processors for the duration of the applicable Service Order; (ii) promptly notifies Client of any subsequent material changes in such authorization; and (iii) downstreams all of its applicable data protection obligations under its Binding Corporate Rules for Processors to Subprocessors by entering into appropriate onward transfer agreements with any such Subprocessors.

EXHIBIT B
(Standard Agreement)
Budget Detail and Payment Provisions

1. INVOICING AND PAYMENT

In consideration of services performed, EDD agrees to compensate the Contractor for services satisfactorily performed in accordance with the SOW, Exhibit A at the rates identified in the Cost Table, Attachment B1. The total dollar shall not exceed **\$10,575,000.00 Ten Million Five Hundred Seventy-Five Thousand Dollars and Zero Cents.**

Invoices shall not be submitted more frequently than monthly. This is a Time and Materials based Agreement, the Contractor's hourly rate may not exceed the rates specified in the Cost Table, Attachment B1. Each invoice must include a certification statement signed by a company official, attesting to the accuracy of the invoice data. Invoices shall include the Contract Number M63734-7100 and shall be submitted in arrears to:

Employment Development Department


Each invoice must include:

- Contract number
- Line item number
- Unit price
- Extended line item price
- Invoice total

2. PAYMENT WITHHOLD

If the EDD rejects all or part of the Contractor's work or work product, EDD shall withhold payment for the rejected work or work product and shall notify the Contractor in writing of the reason(s) why the work or work product was rejected. The Contractor shall take appropriate measures to correct the work and demonstrate to the EDD that the Contractor has successfully completed the work before payment can be made.

3. BUDGET CONTINGENCY

It is mutually understood between the parties that this Agreement may have been written before ascertaining the availability of congressional and legislative appropriation of funds, for the mutual benefit of both parties, in order to avoid program and fiscal delays which would occur if the Agreement were executed after that determination was made.

EXHIBIT B
(Standard Agreement)
Budget Detail and Payment Provisions

This Agreement is valid and enforceable only if (1) sufficient funds are made available by the State Budget Act of the appropriate State Fiscal Year(s) covered by this Agreement for the purposes of this program; and (2) sufficient funds are made available to the State by the United States Government or by the State of California for the Fiscal Year(s) covered by this Agreement for the purposes of this program. In addition, this Agreement is subject to any additional restrictions, limitations or conditions established by the United States Government and/or the State of California, or any statute enacted by the Congress and Legislature, which may affect the provisions, terms or funding of the Agreement in any manner.

The parties mutually agree that if the Congress and/or Legislature does not appropriate sufficient funds for the program, this Agreement shall be amended to reflect any reduction in funds.

4. AVAILABILITY OF FUNDS

If the term of this Agreement covers more than the current fiscal year, continuation of the Agreement is subject to the appropriation of funds by the Legislature. If funds to continue payment are not appropriated, the Contractor agrees to terminate any service supplied to the EDD under this Agreement, and relieve the EDD of any further obligation. The EDD has the option to invalidate the Agreement under the 30-day cancellation clause or to amend the Agreement to reflect any reduction of funds.

**Attachment B-1
(Standard Agreement)
Costs**

Base Agreement Rates

Roles	Hourly Rate	Estimated # of Hours*			Total Cost
		Phase 1	Phase 2	Total Hours	
Program Leadership / Senior Advisor	\$565	2,152.0	3,600.5	5,752.5	\$3,250,162.50
Manager / Senior Specialist	\$425	4,758.0	3,600.5	8,358.5	\$3,552,362.50
Consultant / Specialist	\$285	2,640.0	10,596.75	13,236.75	\$3,772,475.00
					\$10,575,000

* The split of hours between Roles and Phases are estimates for planning purposes only

Contract Extension Rates

If an Extension is exercised, the Parties agree the above Base Agreement Rates, by Role, will be increased each year utilizing an escalation factor equal to the lesser of (a) five percent (5%) per year, or (b) the average change in the Consumer Price Index (CPI-U) during the prior 12 months.

Exhibit C
(Standard Agreement)
GTC 04/2017 – As Modified

1. APPROVAL: This Agreement is of no force or effect until signed by both parties and approved by the Department of General Services, if required. Contractor may not commence performance until such approval has been obtained.
2. AMENDMENT: No amendment or variation of the terms of this Agreement shall be valid unless made in writing, signed by the parties and approved as required. No oral understanding or Agreement not incorporated in the Agreement is binding on any of the parties.
3. ASSIGNMENT: This Agreement is not assignable by the Contractor, either in whole or in part, without the consent of the State in the form of a formal written amendment.
4. AUDIT: Contractor agrees that the awarding department, the Department of General Services, the Bureau of State Audits, or their designated representative shall have the right to review and to copy any records and supporting documentation pertaining to the performance of this Agreement. Contractor agrees to maintain such records for possible audit for a minimum of three (3) years after final payment, unless a longer period of records retention is stipulated. Contractor agrees to allow the auditor(s) access to such records during normal business hours and to allow interviews of any employees who might reasonably have information related to such records. Further, Contractor agrees to include a similar right of the State to audit records and interview staff in any subcontract related to performance of this Agreement. (Gov. Code §8546.7, Pub. Contract Code §10115 et seq., CCR Title 2, Section 1896).
5. INDEMNIFICATION: Contractor agrees to indemnify, defend and save harmless the State, its officers, agents and employees from any and all third party claims and losses accruing or resulting to any and all contractors, subcontractors, suppliers, laborers, and any other person, firm or corporation furnishing or supplying work services, materials, or supplies in connection with the performance of this Agreement, and from any and all third party claims and losses for bodily injury (including death) and damage to real or tangible personal property accruing or resulting to any person, firm or corporation who may be injured or damaged by Contractor in the performance of this Agreement.
6. DISPUTES: Contractor shall continue with the responsibilities under this Agreement during any dispute.

Exhibit C
(Standard Agreement)
GTC 04/2017 – As Modified

7. **TERMINATION FOR CAUSE:** The State may terminate this Agreement and be relieved of any payments should the Contractor fail to perform the requirements of this Agreement at the time and in the manner herein provided and not cure such failure within thirty (30) days after the State provides written notice of such failure to the Contractor. In the event of such termination the State may proceed with the work in any manner deemed proper by the State. All costs to the State shall be deducted from any sum due the Contractor under this Agreement and the balance, if any, shall be paid to the Contractor upon demand.
8. **INDEPENDENT CONTRACTOR:** Contractor, and the agents and employees of Contractor, in the performance of this Agreement, shall act in an independent capacity and not as officers or employees or agents of the State.
9. **RECYCLING CERTIFICATION:** The Contractor shall certify in writing under penalty of perjury, the minimum, if not exact, percentage of post-consumer material as defined in the Public Contract Code Section 12200, in products, materials, goods, or supplies offered or sold to the State regardless of whether the product meets the requirements of Public Contract Code Section 12209. With respect to printer or duplication cartridges that comply with the requirements of Section 12156(e), the certification required by this subdivision shall specify that the cartridges so comply (Pub. Contract Code §12205).
10. **NON-DISCRIMINATION CLAUSE:** During the performance of this Agreement, Contractor and its subcontractors shall not deny the contract's benefits to any person on the basis of race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, genetic information, marital status, sex, gender, gender identity, gender expression, age, sexual orientation, or military and veteran status, nor shall they discriminate unlawfully against any employee or applicant for employment because of race, religious creed, color, national origin, ancestry, physical disability, mental disability, medical condition, genetic information, marital status, sex, gender, gender identity, gender expression, age, sexual orientation, or military and veteran status. Contractor shall insure that the evaluation and treatment of employees and applicants for employment are free of such discrimination. Contractor and subcontractors shall comply with the provisions of the Fair Employment and Housing Act (Gov. Code §12900 et seq.), the regulations promulgated thereunder (Cal. Code Regs., tit. 2, §11000 et seq.), the provisions of Article 9.5, Chapter 1, Part 1, Division 3, Title 2 of the Government Code (Gov. Code §§11135-11139.5), and the regulations or standards adopted by the awarding state agency to implement such article. Contractor shall permit access by representatives of the Department of Fair Employment and Housing and the awarding state agency upon reasonable notice at any time during the normal business hours, but in no case less than 24 hours' notice, to such of its books, records, accounts, and all other sources of information and its facilities as said Department or Agency shall require to ascertain compliance with this clause. Contractor and its subcontractors shall give written

Exhibit C
(Standard Agreement)
GTC 04/2017 – As Modified

notice of their obligations under this clause to labor organizations with which they have a collective bargaining or other agreement. (See Cal. Code Regs., tit. 2, §11105.)

Contractor shall include the nondiscrimination and compliance provisions of this clause in all subcontracts to perform work under the Agreement.

11. CERTIFICATION CLAUSES: The CONTRACTOR CERTIFICATION CLAUSES contained in the document CCC 04/2017 are hereby incorporated by reference and made a part of this Agreement by this reference as if attached hereto.
12. TIMELINESS: Time is of the essence in this Agreement to the extent milestone dates for performance of the Services are specified in this Agreement.
13. COMPENSATION: The consideration to be paid Contractor, as provided herein, shall be in compensation for all of Contractor's expenses incurred in the performance hereof, including travel, per diem, and taxes, unless otherwise expressly so provided.
14. GOVERNING LAW: This contract is governed by and shall be interpreted in accordance with the laws of the State of California.
15. ANTITRUST CLAIMS: The Contractor by signing this agreement hereby certifies that if these services or goods are obtained by means of a competitive bid, the Contractor shall comply with the requirements of the Government Codes Sections set out below.
 - a. The Government Code Chapter on Antitrust claims contains the following definitions:
 - 1) "Public purchase" means a purchase by means of competitive bids of goods, services, or materials by the State or any of its political subdivisions or public agencies on whose behalf the Attorney General may bring an action pursuant to subdivision (c) of Section 16750 of the Business and Professions Code.
 - 2) "Public purchasing body" means the State or the subdivision or agency making a public purchase. Government Code Section 4550.
 - b. In submitting a bid to a public purchasing body, the bidder offers and agrees that if the bid is accepted, it will assign to the purchasing body all rights, title, and interest in and to all causes of action it may have under Section 4 of the Clayton Act (15 U.S.C. Sec. 15) or under the Cartwright Act (Chapter 2 (commencing with Section 16700) of Part 2 of Division 7 of the Business and Professions Code), arising from purchases of goods, materials, or services by the bidder for sale to the purchasing body pursuant to the bid. Such assignment shall be made and become effective

**Exhibit C
(Standard Agreement)
GTC 04/2017 – As Modified**

at the time the purchasing body tenders final payment to the bidder.
Government Code Section 4552.

- c. If an awarding body or public purchasing body receives, either through judgment or settlement, a monetary recovery for a cause of action assigned under this chapter, the assignor shall be entitled to receive reimbursement for actual legal costs incurred and may, upon demand, recover from the public body any portion of the recovery, including treble damages, attributable to overcharges that were paid by the assignor but were not paid by the public body as part of the bid price, less the expenses incurred in obtaining that portion of the recovery. Government Code Section 4553.
 - d. Upon demand in writing by the assignor, the assignee shall, within one year from such demand, reassign the cause of action assigned under this part if the assignor has been or may have been injured by the violation of law for which the cause of action arose and (a) the assignee has not been injured thereby, or (b) the assignee declines to file a court action for the cause of action. See Government Code Section 4554.
16. CHILD SUPPORT COMPLIANCE ACT: For any Agreement in excess of \$100,000, the contractor acknowledges in accordance with Public Contract Code 7110, that:
- a. The contractor recognizes the importance of child and family support obligations and shall fully comply with all applicable state and federal laws relating to child and family support enforcement, including, but not limited to, disclosure of information and compliance with earnings assignment orders, as provided in Chapter 8 (commencing with section 5200) of Part 5 of Division 9 of the Family Code; and
 - b. The contractor, to the best of its knowledge is fully complying with the earnings assignment orders of all employees and is providing the names of all new employees to the New Hire Registry maintained by the California Employment Development Department.
17. UNENFORCEABLE PROVISION: In the event that any provision of this Agreement is unenforceable or held to be unenforceable, then the parties agree that all other provisions of this Agreement have force and effect and shall not be affected thereby.
18. PRIORITY HIRING CONSIDERATIONS: If this Contract includes services in excess of \$200,000, the Contractor shall give priority consideration in filling vacancies in positions funded by the Contract to qualified recipients of aid under Welfare and Institutions Code Section 11200 in accordance with Pub. Contract Code §10353.

Exhibit C
(Standard Agreement)
GTC 04/2017 – As Modified

19. **SMALL BUSINESS PARTICIPATION AND DVBE PARTICIPATION REPORTING REQUIREMENTS:**
- a. If for this Contract Contractor made a commitment to achieve small business participation, then Contractor must within 60 days of receiving final payment under this Contract (or within such other time period as may be specified elsewhere in this Contract) report to the awarding department the actual percentage of small business participation that was achieved. (Govt. Code § 14841.)
 - b. If for this Contract Contractor made a commitment to achieve disabled veteran business enterprise (DVBE) participation, then Contractor must within 60 days of receiving final payment under this Contract (or within such other time period as may be specified elsewhere in this Contract) certify in a report to the awarding department: (1) the total amount the prime Contractor received under the Contract; (2) the name and address of the DVBE(s) that participated in the performance of the Contract; (3) the amount each DVBE received from the prime Contractor; (4) that all payments under the Contract have been made to the DVBE; and (5) the actual percentage of DVBE participation that was achieved. A person or entity that knowingly provides false information shall be subject to a civil penalty for each violation. (Mil. & Vets. Code § 999.5(d); Govt. Code § 14841.)
20. **LOSS LEADER:** If this contract involves the furnishing of equipment, materials, or supplies then the following statement is incorporated: It is unlawful for any person engaged in business within this state to sell or use any article or product as a "loss leader" as defined in Section 17030 of the Business and Professions Code. (PCC 10344(e).)
21. **LIMITATION OF LIABILITY.** The sole liability of either party to the other in relation to any and all claims in any manner related to this Agreement will be for direct damages, not to exceed in the aggregate an amount equal to the total fees paid or payable to Contractor under this Agreement during the 12 month period immediately preceding the event giving rise to the first such claim (or, in respect of any such event occurring during the first 12 months of this Agreement, the fees payable under this Agreement during the first 12 months). In no event will either party be liable for any: (i) consequential, indirect, incidental, special or punitive damages, or (ii) loss of revenue or profits, business interruption, loss of opportunity or anticipated savings, loss of or damage to data, reputational harm or loss of goodwill, or diminution in stock price or enterprise value (whether directly or indirectly arising).
22. **STATE RESPONSIBILITIES.** To the extent that the State fails to perform any of its responsibilities described in this Agreement, Contractor (i) shall be excused from

Exhibit C
(Standard Agreement)
GTC 04/2017 – As Modified

failure to perform any affected obligations under this Agreement, (ii) shall be entitled to a reasonable extension of time considering the particular circumstances, and, if agreed by the parties, a reasonable reimbursement of additional costs incurred as a result, and (iii) shall not be responsible for any consequence or liability arising from the State's failure. Each party will notify the other as promptly as practicable after becoming aware of the occurrence of any such condition.

23. NAME. Neither party will use the other party's name outside its organization without prior written consent of the other party.
24. THIRD PARTY BENEFICIARIES. There are no third party beneficiaries to this Agreement.

EXHIBIT D
(Standard Agreement)
Protection of Confidentiality

Federal and state confidentiality laws, regulations, and administrative policies classify all the Employment Development Department (EDD) information provided under this Agreement as confidential. The federal and state laws prohibit disclosure of the EDD's confidential information to the public and mandate its protection against loss and against unauthorized access, use, disclosure, modification, or destruction.

Accenture LLP, must therefore, agree to the following security and confidentiality requirements:

I. ADMINISTRATIVE SAFEGUARDS

- a. Adopt policies and procedures, as applicable, to ensure use of the EDD's confidential information solely for purposes specifically authorized under this Agreement that meet the requirements of Title 20, Code of Federal Regulations §603.10.
- b. Warrant by execution of this Agreement, that no person or selling agency has been employed or retained to solicit or secure this Agreement upon agreement or understanding for a commission, percentage, brokerage, or contingent fee. In the event of a breach or violation of this warranty, the EDD shall have the right to annul this Agreement without liability, in addition to other remedies provided by law.
- c. Warrant and certify that in the performance of this Agreement Accenture LLP, will comply with all applicable statutes, rules and/or regulations, and Agreement information security requirements, including but not limited to the following:
 - **California Unemployment Insurance Code §1094** (Disclosure Prohibitions)
 - **Title 20, Code of Federal Regulations §603.9 and §603.10** (Federal Unemployment Compensation Safeguards and Security Requirements)
 - **California Civil Code §1798, et seq.** (Information Practices Act)
 - **California Penal Code §502** (Computer Fraud Act)
 - **Title 5, U.S. Code §552a** (Federal Privacy Act Disclosure Restrictions)
 - **Title 42, U.S. Code §503** (Social Security Act)
 - **Title 18, U.S. Code §1905** (Disclosure of Confidential Information)
- d. Except for state agencies, agree to indemnify the EDD against any third party loss, cost, damage or liability to the extent caused by Accenture's violations of these applicable statutes, rules and/or regulations, and Agreement information security requirements.
- e. Protect the EDD's information residing in or on Accenture's internal systems and in Accenture's physical possession against unauthorized access, at all times, in all forms of media. Access and use the information obtained under this Agreement only to the extent necessary to assist in the valid administrative needs of the program receiving such information, and only for the purposes defined in this Agreement.
- f. Keep all the EDD's confidential information completely confidential. Make this information available to authorized personnel on a "need-to-know" basis and only for the purposes authorized under this Agreement. "Need-to-know" refers to those authorized personnel who need information to perform their official duties in connection with the use of the information authorized by this Agreement.

EXHIBIT D
(Standard Agreement)
Protection of Confidentiality

- g. Notify the EDD Help Desk at (916) 654-1010, immediately upon confirmed discovery, that there has been a breach in security which has or may have resulted in compromise to the EDD confidential information. For purposes of this section, immediately is defined within 24 hours of confirmed discovery of the breach of EDD confidential data. The notification shall be by phone and email. **It is not sufficient to simply leave a message.** The notification must include a detailed description of the incident (such as time, date, location, and circumstances) and identify responsible personnel (name, title and contact information). The verbal notification shall be followed with an email notification to [REDACTED]

II. MANAGEMENT SAFEGUARDS

- a. Acknowledge that the confidential information obtained by Accenture LLP, under this Agreement remains the property of the EDD.
- b. Instruct all personnel assigned to work with the information provided under this Agreement regarding the following:
- Confidential nature of the EDD information.
 - Requirements of this Agreement.
 - Sanctions specified in federal and state unemployment compensation laws and any other relevant statutes against unauthorized disclosure of confidential information provided by the EDD.
- c. Require that all personnel assigned to work with the information provided by the EDD complete the EDD Confidentiality Agreement (Attachment D-1):
- d. Return the following completed documents to the EDD Contract Services Group:

The EDD Indemnity Agreement (Attachment D-2): Required to be completed by the Accenture LLP, Chief Financial Officer or authorized Management Representative, unless Accenture LLP, is a State Agency.

- The EDD Statement of Responsibility Information Security Certification (Attachment D-3): Required to be completed by the Information Security Officer or authorized Management Representative.
- e. Permit the EDD to make on-site inspections to ensure that the terms of this Agreement are being met. Make available to the EDD staff, on request and during on-site reviews, copies of the EDD Confidentiality Agreement (Attachment D-1) completed by personnel assigned to work with the EDD's confidential information, and hereby made a part of this Agreement.

EXHIBIT D
(Standard Agreement)
Protection of Confidentiality

- f. Maintain a system of records sufficient to allow an audit of compliance with the requirements under subsection (d) of this part. Once per 12 sequential calendar months, EDD may request Accenture LLP in writing to complete an information security and physical security assessment questionnaire. Accenture LLP agrees to respond to such questionnaire as soon as commercially reasonable. To the extent Accenture LLP performs and makes available to Customers an independent third-party assessment or certification with respect to that service (e.g., SOC 2), upon EDD'S request, EDD may review an available summary of the results of such security assessment for the services containing EDD Materials.

III. USAGE, DUPLICATION, AND REDISCLOSURE SAFEGUARDS

- a. Use the EDD's confidential information only for purposes specifically authorized under this Agreement. The information is not admissible as evidence in any action or special proceeding except as provided under §1094(b) of the California Unemployment Insurance Code (CUIC). Section 1095(u) of the CUIC does not authorize the use of the EDD's confidential information by any private collection agency.
- b. Extraction or use of the EDD information for any purpose outside the purposes stated in this Agreement is strictly prohibited. The information obtained under this Agreement shall not be reproduced, published, sold, or released in original or any other form not specifically authorized under this Agreement.
- c. Disclosure of any of the EDD information to any person or entity not specifically authorized in this Agreement is strictly prohibited. Personnel assigned to work with the EDD's confidential information shall not reveal or divulge to any person or entity any of the confidential information provided under this Agreement except as authorized or required by law.

IV. PHYSICAL SAFEGUARDS

- a. Take precautions to ensure that only authorized personnel are given access to physical, electronic and on-line files. Store electronic and hard copy information in a place physically secure from access by unauthorized persons. Process and store information in electronic format, such as magnetic tapes or discs, in such a way that unauthorized persons cannot retrieve the information by means of computer, remote terminal, or other means.
- b. Store all the EDD's confidential documents in a physically secure manner at all times to prevent unauthorized access.
- c. Store the EDD's confidential electronic records in a secure central computer facility. Where in-use on a shared computer system or any shared data storage system, ensure appropriate information security protections are in place. Accenture LLP, shall ensure that appropriate security access controls, storage protections and use restrictions are in place to keep the confidential information in the strictest confidence and shall make the information available to its own personnel on a "need-to-know" basis only.
- d. Store the EDD's confidential data in encrypted format when recorded on removable electronic storage media, or on mobile computing devices, such as a laptop computer.

EXHIBIT D
(Standard Agreement)
Protection of Confidentiality

- e. Maintain an audit trail and record data access of authorized users and authorization level of access granted to the EDD's data, based on job function.
- f. Direct all personnel permitted to use the EDD's data to avoid leaving the data displayed on their computer screens where unauthorized users may view it. Personnel should retrieve computer printouts as soon as they are generated so that the EDD's data is not left unattended in printers where unauthorized personnel may access them.
- g. Dispose of confidential information obtained from the EDD, and any copies thereof made by Accenture LLP, after the purpose for which the confidential information is disclosed is served. Disposal means return of the confidential information to the EDD or destruction of the information utilizing an approved method of confidential destruction, which includes electronic deletion (following Department of Defense specifications) shredding, burning, or certified or witnessed destruction.



EDD Contract No. M63734-7100
EDD/Accenture LLP
ATTACHMENT NO. D1
Page 1 of 1

EMPLOYMENT DEVELOPMENT DEPARTMENT CONFIDENTIALITY AGREEMENT

Information resources maintained by the State of California Employment Development Department (EDD) and provided to your agency may be confidential or sensitive. Confidential and sensitive information are not open to the public and require special precautions to protect it from wrongful access, use, disclosure, modification, and destruction. The EDD strictly enforces information security. If you violate these provisions, you may be subject to administrative, civil, and/or criminal action.

an employee of

Accenture LLP

PRINT YOUR NAME

PRINT YOUR EMPLOYER'S NAME

hereby acknowledge that the confidential and/or sensitive records of the Employment Development Department are subject to strict confidentiality requirements imposed by state and federal law include the California Unemployment Insurance Code (UIC) §§1094 and 2111, the California Civil Code (CC) §1798 et seq., the California Penal Code (PC) §502, Title 5, USC §552a, Code of Federal Regulations, Title 20 part 603, and Title 18 USC §1905.

INITIAL acknowledge that my supervisor and/or the Contract's Confidentiality and Data Security Monitor reviewed with me the confidentiality and security requirements, policies, and administrative processes of my organization and of the EDD.

INITIAL acknowledge responsibility for knowing the classification of the EDD information I work with and agree to refer questions about the classification of the EDD information (public, sensitive, confidential) to the person the Contract assigns responsibility for the security and confidentiality of the EDD's data.

INITIAL acknowledge responsibility for knowing the privacy, confidentiality, and data security laws that apply to the EDD information I have been granted access to by my employer, including UIC §§1094 and 2111, California Government Code § 15619, CC § 1798.53, and PC § 502.

INITIAL acknowledge that wrongful access, use, modification, or disclosure of confidential information may be punishable as a crime and/or result in disciplinary and/or civil action taken against me including but not limited to: reprimand, suspension without pay, salary reduction, demotion, or dismissal and/or fines and penalties resulting from criminal prosecution or civil lawsuits, and/or termination of contract.

INITIAL acknowledge that wrongful access, inspection, use, or disclosure of confidential information for personal gain, curiosity, or any non-business related reason is a crime under state and federal laws.

INITIAL acknowledge that wrongful access, use, modification, or disclosure of confidential information is grounds for immediate termination of my organization's Contract with the EDD.

INITIAL agree to protect the following types of the EDD confidential and sensitive information:

- | | |
|-------------------------|---|
| • Wage Information | • Applicant Information |
| • Employer Information | • Proprietary Information |
| • Claimant Information | • Operational Information (manuals, guidelines, procedures) |
| • Tax Payer Information | |

INITIAL hereby agree to protect the EDD's information on either paper or electronic form by:

- Accessing or using the EDD supplied information only as specified in the Contract for the performance of the specific work I am assigned.
- Never accessing information for curiosity or personal reasons.
- Never showing or discussing sensitive or confidential information to or with anyone who does not have the need to know.
- Placing sensitive or confidential information only in approved locations.
- Never removing sensitive or confidential information from the work site without authorization.
- Following encryption requirements for all personal, sensitive, or confidential information in any portable device or media.

"I certify that I have read and initialed the confidentiality statements printed above and will abide by them."

Print Full Name (last, first, MI)

Signature

Print Name of Requesting Agency

Date Signed

Check the appropriate box:

- | | |
|--|------------------------------------|
| <input type="checkbox"/> Employee | <input type="checkbox"/> Student |
| <input type="checkbox"/> Subcontractor | <input type="checkbox"/> Volunteer |
| <input type="checkbox"/> Other | |

Explain



EDD Contract No. M63734-7100
EDD/Accenture LLP
ATTACHMENT No. D2
Page 1 of 1

EMPLOYMENT DEVELOPMENT DEPARTMENT INDEMNITY AGREEMENT

In consideration of access to the EDD information which is personal, sensitive, or confidential,

Accenture LLP

(Enter Requesting Agency/Entity Name)

agrees to indemnify the EDD against any and all liability costs, damages, attorney fees, and other expenses the EDD may incur by reason of or as a result of any unauthorized use of the personal, sensitive, or confidential information or any violation of the "Confidentiality Agreement" by any and all employees of:

Accenture LLP

(Enter Requesting Agency/Entity Name)

This obligation shall be continuous and may not be changed or modified unless agreed to in writing.

In addition, I understand that the following penalties may be incurred for any such misuse of the EDD Information:

1. Any individual who has access to returns, reports, or documents maintained by the EDD who fails to protect the confidential information from being published or open to the public may be punished by imprisonment in the county jail for up to one year or a fine of \$20,000.00 or both. (California Unemployment Insurance Code §§ 2111 and 2122).
2. Any person who intentionally discloses information, not otherwise public, which they knew or should have known was obtained from personal information maintained by a state agency, shall be subject to civil action for invasion of privacy by the individual to whom the information pertains. (California Civil Code §1798.53).
3. Any unauthorized access to the EDD computer data, computer systems, or unauthorized use of the EDD data is punishable by a fine or imprisonment in the county jail or both. (California Penal Code §502).

I certify that I have read, understand, and agree with the above terms.

SIGNED BY REQUESTING ENTITY REPRESENTATIVE



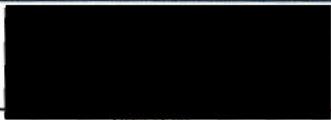
Print Full Name

As 

Print Title

Accenture LLP

Print Name of Requesting Entity



Signature

May 1, 2021

Date Signed

Enter Name Governmental Sponsor/Entity



EDD Contract No. M63734-7100
 EDD/Accenture LLP
ATTACHMENT No. D3
 Page 1 of 1

EMPLOYMENT DEVELOPMENT DEPARTMENT STATEMENT OF RESPONSIBILITY

INFORMATION SECURITY CERTIFICATION

We, the Information Security Officer and <Enter title of authorized official: Agency Chief Information Officer, Confidentiality Officer, Disclosure Officer, or other individual with delegated signature authority> hereby certify that Accenture, LLP has in place the safeguards and security requirements stated in this Agreement. We therefore accept responsibility for ensuring compliance with these requirements, as set forth in Exhibit "D" of the EDD Contract No. M63734-7100

<div style="background-color: black; width: 150px; height: 40px; margin: 0 auto;"></div> <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/> INFORMATION SECURITY OFFICER SIGNATURE	<div style="background-color: black; width: 150px; height: 40px; margin: 0 auto;"></div> <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/> PROGRAM DIRECTOR OR CHIEF INFORMATION OFFICER SIGNATURE
<div style="background-color: black; width: 100px; height: 20px; margin: 0 auto;"></div> <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/> PRINT NAME OF INFORMATION SECURITY OFFICER	<div style="background-color: black; width: 100px; height: 20px; margin: 0 auto;"></div> <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/> PRINT NAME
<div style="background-color: black; width: 150px; height: 20px; margin: 0 auto;"></div> <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/> PRINT TITLE	<div style="background-color: black; width: 150px; height: 20px; margin: 0 auto;"></div> <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/> PRINT TITLE
<div style="background-color: black; width: 100px; height: 20px; margin: 0 auto;"></div> <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/> TELEPHONE NUMBER	<div style="background-color: black; width: 100px; height: 20px; margin: 0 auto;"></div> <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/> TELEPHONE NUMBER
<div style="background-color: black; width: 250px; height: 20px; margin: 0 auto;"></div> <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/> E-MAIL ADDRESS	<div style="background-color: black; width: 250px; height: 20px; margin: 0 auto;"></div> <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/> E-MAIL ADDRESS
<div style="background-color: black; width: 100px; height: 20px; margin: 0 auto;"></div> <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/> May 1, 2021 DATE SIGNED	<div style="background-color: black; width: 100px; height: 20px; margin: 0 auto;"></div> <hr style="border: 0; border-top: 1px solid black; margin: 5px 0;"/> May 1, 2021 DATE SIGNED

NOTE: Return this Information Security Certification to the EDD Contract Manager with the signed copies of the Contract.

FOR THE EDD USE ONLY

1. Information Security Certification received by:

<hr style="border: 0; border-top: 1px solid black; margin-bottom: 5px;"/> EDD CONTRACT MANAGER NAME	<hr style="border: 0; border-top: 1px solid black; margin-bottom: 5px;"/> DATE RECEIVED
---	---

2. The EDD information asset access approved by:

<hr style="border: 0; border-top: 1px solid black; margin-bottom: 5px;"/> CONTRACT MANAGER OR DISCLOSURE COORDINATOR	<hr style="border: 0; border-top: 1px solid black; margin-bottom: 5px;"/> DATE APPROVED (AFF, EMAIL, ETC.)
--	--

NOTE: The EDD must have a signed "Information Security Certification" in its possession prior to disclosure of any personal, confidential, or sensitive information to Accenture LLP

EXHIBIT E
(Standard Agreement)
Safeguarding Contract Language Administrative Requirements

The following administrative requirements must be completed before services are performed in accordance with the Contract. The Contractor is responsible for any costs or expenses related to time for completing these items. The Employment Development Department (EDD) may terminate the Contract and be relieved of any payments should the Contractor fail to perform the requirements of the Background Investigation at the time and in the manner described below:

a. Background Investigation

Pursuant to Government Code section 1044, the EDD shall conduct a background investigation of the Contractor, its employees, contractors, agents, volunteers, vendors, or subcontractors who will have access to Federal Tax Information (FTI) as part of their duties under this Agreement; and reserves the right to disapprove any individual from performing services under the scope of this Agreement. The Background Investigation will include fingerprinting and an inquiry to the California Department of Justice (DOJ) and the Federal Bureau of Investigations (FBI) to disclose Criminal Offender Record Information (CORI). Investigations are conducted to ascertain whether a Contractor, its employees, contractors, agents, volunteers, vendors, or subcontractors have any state or federal convictions, or are currently released from custody on bail or on their own recognizance pending trial.

Each Contractor, its employees, contractors, agents, volunteers, vendors, or subcontractors who are to perform services under this Agreement must voluntarily consent to a Background Investigation. Fingerprint rolling fees and Background Investigation costs will be borne by the EDD if the preferred fingerprint rolling vendor is utilized. If the Contractor, its employees, contractors, agents, volunteers, vendors, or subcontractors choose to go to a non-preferred Live Scan fingerprint vendor, the costs will be borne by the Contractor, payable at the time of fingerprinting and will not be reimbursed by the EDD. Previous clearances and/or investigations conducted by other agencies will not be accepted as an alternative to the EDD's Background Investigation.

Once this Contract is awarded, it is the responsibility of the Contractor to provide a list of names of individuals who will be working on site at an EDD location or working remotely with access to EDD information (data) and/or information assets (servers, workstations, routers, switches, printers, etc.) to the Contract Monitor. The Contractor will be provided BCIA 8016 forms for its employees, contractors, agents, volunteers, vendors, or subcontractors to utilize for their fingerprint rolling at an EDD preferred fingerprint rolling vendor. The EDD will receive the CORI reports from DOJ and evaluate the information provided against the EDD's established criteria. The Contractor, its employees, contractors, agents, volunteers, vendors, or subcontractors must successfully pass a background investigation pursuant to the EDD's criteria prior to the EDD issuing a badge or access to the EDD's data.

Within 5 business days, the Contractor shall notify the EDD Contract Monitor when its employee, contractor, agent, volunteer, vendor, or subcontractor, working under this Agreement is terminated, not hired, or reassigned to other work. Within 5 business days, the Contractor shall notify the EDD Contract Monitor when its new employee, contractor, agent, volunteer, vendor, or subcontractor is assigned to work under this Agreement in order for the EDD to commence conducting a background investigation of its new employee, contractor, agent, volunteer, vendor, or subcontractor.

EXHIBIT E
(Standard Agreement)
Safeguarding Contract Language Administrative Requirements

b. Annual Information Security Awareness and Privacy Training

California state policy requires that the EDD must provide for the proper use and protection of its information assets and arrange for basic security and privacy awareness training (SAM sections 5305.1, 5320.1, 5320.2, 5320.3, SIMM 5330-B) for new users and annually thereafter. Therefore, the Contractor, its employees, contractors, agents, volunteers, vendors, or subcontractors who access state resources must complete the designated EDD online annual Information Security Awareness and Privacy Training prior to accessing EDD information assets and/or beginning work on a contract. The EDD University will set up a training account. While the training course is provided by the EDD, any expenses, including Contractor time, related to new and/or annual Information Security Awareness and Privacy Training will be the responsibility of the Contractor.

EXHIBIT F
(Standard Agreement)
Safeguarding Contract Language for Technology Services

I. PERFORMANCE

In performance of this Contract, the Contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

- (1) All work will be done under the supervision of the Contractor or the Contractor's employees.
- (2) The Contractor and the Contractor's employees, Contractors, agents, volunteers, vendors, or subcontractors must meet the background check requirements provided in Exhibit E of this Contract.
- (3) Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this Contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this Contract. Disclosure to anyone other than an officer or employee of the Contractor will be prohibited.
- (4) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.
- (5) The Contractor certifies that the data processed during the performance of this Contract will be completely purged from all data storage components of his or her computer facility, and no output will be retained by the Contractor at the time the work is completed. If immediate purging of all data storage components is not possible, the Contractor certifies that any Internal Revenue Service (IRS) data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.
- (6) Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used.
- (7) All computer systems receiving, processing, storing or transmitting federal tax information (FTI) must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to FTI.
- (8) No work involving FTI furnished under this Contract will be subcontracted without prior written approval of the IRS.

EXHIBIT F
(Standard Agreement)
Safeguarding Contract Language for Technology Services

- (9) The Contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office. (See Section 10.0, Reporting Improper Inspections or Disclosures of the IRS Publication 1075.) The agency will have the right to void the Contract if the Contractor fails to provide the safeguards described above.

II. CRIMINAL/CIVIL SANCTIONS

- (1) Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth in 26 C.F.R. § 301.6103(n)-1.
- (2) Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this Contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the Contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for Federal employees] in an amount equal to the sum of the greater of \$1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC 7213A and 7431 and set forth in 26 C.F.R. § 301.6103(n)-1.
- (3) Additionally, it is incumbent upon the Contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C.

EXHIBIT F
(Standard Agreement)
Safeguarding Contract Language for Technology Services

§ 552(a). Specifically, 5 U.S.C. § 552(a)(i)(1), which is made applicable to Contractors by 5 U.S.C. § 552(a)(m)(1), provides that any officer or employee of a Contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

- (4) Granting a Contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain their authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, Contractors must be advised of the provisions of IRCs 7431, 7213, and 7213A. (See Exhibit 4, Sanctions for Unauthorized Disclosure, and Exhibit 5, Civil Damages for Unauthorized Disclosure of the IRS Publication 1075). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10.0, Reporting Improper Inspections or Disclosures of the IRS Publication 1075.) For both the initial certification and the annual certification, the Contractor must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and the agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the Contractor to inspect facilities and operations performing any work with FTI under this Contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual and/or automated scanning tools to perform compliance and vulnerability assessments of information technology assets that access, store, process or transmit FTI. On the basis of such inspection, corrective actions may be required in cases where the Contractor is found to be noncompliant with Contract safeguards.

* Language used throughout Exhibit F is derived from IRS Publication 1075

EXHIBIT G
(Standard Agreement)
Special Terms and Conditions

1. LOBBYING RESTRICTIONS

The Contractor must certify lobbying activities and disclose lobbying activities by completing the Certification Regarding Lobbying and Disclosure of Lobbying Activities and submit it with the Offer. The forms shall be completed by the reporting entity, whether sub-awardee or prime Federal recipient, at the initiation or receipt of a covered Federal action, or a material change to a previous filing, pursuant to title 31 U.S.C. Section 1352.

2. CERTIFICATION REGARDING DEBARMENT

Debarment, suspension, ineligibility and voluntary exclusion of lower tier covered transaction certification is required for this procurement by the regulations implementing Executive Order 12549, Debarment and Suspension, 29 CFR Part 98, Section 98.510, participants' responsibilities. The regulations were published as Part VII of the May 26, 1988, Federal Register (Pages 19160-19211).

3. WORKFORCE INNOVATION AND OPPORTUNITY ACT

Contractor agrees to conform to the nondiscrimination provisions of the Workforce Innovation and Opportunity Act (WIOA) and other federal nondiscrimination requirements as referenced in 29 CFR, Part 37 and 38.

4. PUBLIC CONTRACT CODE

The Contractor is advised that he/she has certain duties, obligations, and rights under the Public Contract Code §§ 10335 – 10381 and 10410 - 10412, with which the Contractor should be familiar. These Public Contract Code sections can be viewed at:

http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=PCC§ionNum=10335

http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=PCC§ionNum=10381

http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=PCC§ionNum=10410

5. NOTICES

All notices relating to this Contract shall be in writing and shall be sent to the respective Contract Managers set forth in this Contract. All such notices shall be deemed delivered if deposited, postage prepaid, in the United States mail and sent to the parties' last known address.

EXHIBIT G
(Standard Agreement)
Special Terms and Conditions

6. AVOIDANCE OF CONFLICTS OF INTEREST BY CONTRACTOR

- A. Consultants are advised that that Political Reform Act prohibits public officials, which include consultants, from making, participating in making, or in any way attempting to use his official position to influence a governmental decision in which he knows or has reason to know he has a financial interest. (Government Code § 87100; see Government Code § 81000 and Government Code § 1090 et seq.). For purposes of this contract, consultants are defined as any individual performing work under this contract.
- B. The Contractor shall make all reasonable efforts to ensure that no conflict of interest exists between its officers, agents, employees, consultants or members of its governing body.
- C. The Contractor shall prevent its officers, agents, employees, consultants or members of its governing body from using their positions for purposes that are, or give the appearance of being, motivated by a desire for private gain for themselves or others such as those with whom they have family, business, or other ties.
- D. During the performance of this contract, should the Contractor become aware of a financial conflict of interest that may foreseeably allow an individual or organization involved in this Contract to materially benefit from the State's adoption of an action(s) recommended as a result of this contract, the Contractor must inform the State in writing within 10 working days.
- E. Failure to disclose a relevant financial interest on the part of the consultant will be deemed grounds for termination of the Contract with all associated costs to be borne by the Contractor and, in addition, the Contractor may be excluded from participating in the State's bid processes for a period of up to 360 calendar days in accordance with the Public Contract Code section 12102(j).
- F. The EDD may request additional information regarding a consultant's economic interests. If the additional information is not provided to the satisfaction of the EDD, then the Contractor must provide a substitute consultant with similar credentials to resolve the potential conflict as provided in paragraph D.
- G. Consultants are advised that the Fair Political Practices Commission has jurisdiction to enforce the Political Reform Act and may seek civil and criminal prosecution for violations of the act, including failure to disclose financial interests. Other penalties for violating the Political Reform Act could include fines, conviction of a misdemeanor, disqualification from serving in public office or as a lobbyist, and being responsible for the costs of the litigation, including attorney's fees.
- H. All consultants providing work under this Contract shall include a completed Statement of Economic Interests, Form 700 (<https://www.fppc.ca.gov/Form700.html>) at the time of award. In addition, consultants shall file a Form 700 annually by April 1, thereafter during the life of the contract. Each new and/or substitute consultant shall file a Form 700 prior to performing any work on the contract.

EXHIBIT G
(Standard Agreement)
Special Terms and Conditions

- I. Consultants are advised that they may amend their Form 700 at any time and that amending an incorrect or incomplete report may be considered evidence of good faith by the Fair Political Practices Commission.

7. DISPUTES

Any dispute concerning a question of fact arising under the term of this Contract which is not disposed of within a reasonable period of time (ten days) by the Contractor and State employees normally responsible for the administration of this contract shall be brought to the attention of the Chief Executive Officer (or designated representative) of each organization for joint resolution.

8. SUBCONTRACTOR LANGUAGE

Nothing contained in this Contract shall create any contractual relationship between the State and any subcontractor, and no subcontract shall relieve the Contractor of its responsibilities and obligations hereunder. The Contractor is fully responsible to the State for the act and omissions of its subcontractor and of persons either directly or indirectly employed by any of them.

The Contractor's obligation to pay its subcontractors is independent from the State's obligation to make payment to the Contractor. As a result, the State shall have no obligation to pay or to enforce the payment of any moneys to any subcontractor.

9. BACKGROUND INVESTIGATION

The EDD shall conduct a background investigation of the Contractor, its employees, contractors, agents, volunteers, vendors, or subcontractors, unless the EDD determines such individuals are not subject to a background investigation. Individuals must voluntarily consent to a background check and the EDD reserves the right to disapprove any individual from performing services under the scope of the Contract.

Investigations will be conducted to ascertain whether a Contractor, its employees, contractors, agents, volunteers, vendors, or subcontractors have any state or federal convictions, or are currently released from custody on bail or on their own recognizance pending trial. The background investigation will include fingerprinting and an inquiry to the California Department of Justice (DOJ) and the Federal Bureau of Investigations (FBI) to disclose Criminal Offender Record Information (CORI). The EDD will absorb the cost of the fingerprinting services.

10. EVALUATION OF CONTRACT/CONTRACTOR

For IT Services over \$500,000, within sixty (60) days after the completion of the Contract, the Program Manager shall complete a written evaluation of Contractor's performance under the Contract. A copy of the STD 971 must be emailed to the State Department of Technology at form971@state.ca.gov and shall remain in the contract file for 36 months. If the Contractor did not satisfactorily perform the work, a copy of the evaluation form will be sent to the Contractor within fifteen (15) working days of the completion of the evaluation. (PCC

EXHIBIT G
(Standard Agreement)
Special Terms and Conditions

12102.3). You may view the form
here: <https://www.documents.dgs.ca.gov/dgs/fmc/pdf/std971.pdf>

11. CONTRACTOR STAFF CHANGES

The Contractor reserves the sole right to determine the assignment of its employees. The Contractor agrees to notify EDD in writing of all changes in personnel assigned to this Contract as soon as is practicable.

The Contractor agrees that if EDD determines that Contractor personnel are failing to adequately perform services, the Contractor shall provide substitute personnel that meet or exceed all minimum qualifications as stated in this Contract.

The Contractor agrees that if Contractor personnel assigned to the project are unable to perform their duties due to illness, resignation, or other factors beyond the Contractor's control, the Contractor shall provide substitute personnel that meet or exceed all minimum qualifications as stated in this Contract.

12. OWNERSHIP RIGHTS

All data, documents, software and other artifacts produced under the contract become the sole property of EDD with an exception for preexisting materials (including modifications and derivatives thereof) to remain owned by the Contractor. Each part is free to use concepts, techniques and know-how retained in the unaided memories of those involved in performance or receipt of the services.