STATE OF CALIFORNIA DEPARTMENT OF GENERAL SERVICE
SOFTWARE LICENSING PROGRAM (SLP)
CONTRACT NO. SLP-22-70-0027O
ALLIED NETWORK SOLUTIONS INC

APPROVED:
CITY OF MERCED
A California Charter Municipal Corporation

BY:_____
D. Scott McBride
City Manager

ATTEST:
D. SCOTT MCBRIDE, CITY CLERK

BY:_____
Assistant/Deputy City Clerk

APPROVED AS TO FORM:
CRAIG J. CORNWELL, CITY ATTORNEY

BY: Craig Cornwell 4-23-2026
City Attorney Date

ACCOUNT DATA:
M. VENUS RODRIGUEZ

BY: _____
Verified by Finance Officer

DGS CALIFORNIA DEPARTMENT OF GENERAL SERVICES

Procurement Division
707 Third Street, 2nd Floor, MS #2-202
West Sacramento, CA 95605-2811

State of California
SOFTWARE LICENSING PROGRAM (SLP) AGREEMENT AMENDMENT NO. 3

softwarelicensingprogram

Contractor:	Allied Network Solutions, Inc
Contract Number:	SLP-22-70-0027O
SLP Contract Term:	01/01/2022 through 12/31/2027
Contract Base:	Red Hat, Inc. Offer Number RedHat-SLP-2022

This amendment is being issued to:

- Extend the term of this SLP agreement through 12/31/2027
- All other terms and conditions remain the same.

For State of CA:

Kimberley Hettrick Digitally signed by Kimberley Hettrick Date: 2025.09.23 13:33:32 -07'00'

For Stephanne Lim
Manager
Multiple Award Programs Section
Procurement Division
Department of General Services

9/23/25
Date

For Contractor:

Signature

President/CEO
Printed Title

Roger Schnorenberg
Printed Name

Allied Network Solutions, Inc.
Company Name

September 12, 2025
Date

DGS CALIFORNIA DEPARTMENT OF GENERAL SERVICES

Procurement Division
707 Third Street, 2nd Floor, MS #2-202
West Sacramento, CA 95605-2811

State of California
SOFTWARE LICENSING PROGRAM (SLP)
AMENDMENT NO. 2

softwarelicensingprogram

Contractor	Allied Network Solutions, Inc
Contract Number:	SLP-22-70-0027O
SLP Contract Term:	1/1/2022 through 12/31/2025
Contract Base:	Red Hat Offer Number RedHat-SLP-2022

This amendment is being issued to:

1. Remove all incorporated references to the state's general and special provisions and replace with the following provisions:

   - Information Technology - General Provisions - Cloud Computing Services, DGS PD 402-ITGP (Cloud), effective 02/20/2025
   - Information Technology - General Provisions - Non-Cloud Goods & Services, DGS PD 403-ITGP (Non-Cloud), effective 02/20/2025

2. Remove the provision "GENERATIVE ARTIFICIAL INTELLIGENCE (GENAI) REPORTING" and replace with the following provision:

   GENERATIVE ARTIFICIAL INTELLIGENCE (GENAI)

   State agencies must follow the required GenAI purchase procedures outlined in the State Contracting Manual (SCM) and the California Department of Technology GenAI policies.

ALL OTHER TERMS AND CONDITIONS REMAIN THE SAME.

For State of CA:

For Julie Matthews Digitally signed by Julie Matthews Date: 2025.06.18 17:06:03 -07'00'

Stephanne Lim
Manager
Multiple Award Programs Section
Procurement Division
Department of General Services

6/18/2025
Date

For Contractor:

Signature

President/CEO
Printed Title

Roger Schnorenberg
Printed Name

Allied Network Solutions, Inc.
Company Name

May 2, 2025
Date

DGS CALIFORNIA DEPARTMENT OF GENERAL SERVICES

Procurement Division
707 Third Street, 2nd Floor, MS #2-202
West Sacramento, CA 95605-2811

State of California
SOFTWARE LICENSING PROGRAM (SLP)

softwarelicensingprogram

Contractor:	Allied Network Solutions, Inc.
Contract Number:	SLP-22-70-0027O
SLP Contract Term:	01/01/2022 through 12/31/2025
Contract Base:	Red Hat Offer Number RedHat-SLP-2022

This contract is available for use by State of California departments and any city, county, special district, educational agency, local government body or corporation empowered to expend public funds. While the state makes this contract available, each local agency should make its own determination whether the SLP is consistent with their procurement policies and regulations.

The SLP Contractor is required to provide all SLP contract terms and conditions with the list of products, services and prices.

Terms and conditions listed below are hereby incorporated by reference and made a part of this SLP Agreement as if attached herein and shall apply to the purchase of goods or services made under this Participating Agreement. Contractor non-compliance with the requirements of this contract may result in contract termination.

By signing below, Contractor agrees to the General Provisions dated November 19, 2021, SaaS Cloud Computing Services Special Provisions dated March 15, 2018 and all other provisions included herein.

1) General Provisions – Information Technology (GSPD-401IT) effective 11/19/2021
2) Cloud Computing Services Special Provisions (Software as a Service) effective 3/15/2018
3) General Provisions – Information Technology Cloud Computing Software as a Service (SaaS) effective 11/19/2021
4) Cloud Computing Special Provisions for Infrastructure as a Service (Iaas) & Platform as a Service (Paas) effective 05/11/16

For State of CA:

Original Signature on File

Patrick Mullen
Manager
Multiple Award Programs Section
Procurement Division
Department of General Services

Date

For Contractor:

Original Signature on File

Signature

Printed Title

Printed Name

Company Name

Date

CONTRACTOR PROVIDES COPY OF THE CONTRACT AND SUPPLEMENTS

The SLP Contractors are required to provide the entire contract that consists of the following:

- SLP Cover sheet with signatures from the DGS Procurement Division Deputy Director or designee and Contractor.
- Ordering instructions.
- Std. 204 Payee Data Record.
- SLP Contract terms and conditions (General provisions).
- Software License Agreement pricing.
- Supplements, if applicable

CONTRACTOR QUARTERLY REPORTS

Contractors are required to submit a detailed report quarterly to the DGS Procurement Division, Software Licensing Program. A separate report is required for each contract, as differentiated by alpha suffix (if applicable). Contractors with resellers are responsible for reporting reseller ordering activity. Any report that does not follow the required format or that excludes information will be deemed incomplete and returned to the contractor.

All SLP contractors, including certified Small Businesses and Disabled Veteran Business Enterprises, will be required to pay DGS-PD a 1.25% incentive fee for all orders placed by local government agencies via a SLP contract. This policy however, does not affect orders placed by State government offices. State agencies will continue to be billed the applicable administrative use fee by the DGS-PD.

The SLP Quarterly Business Activity Report form separates sales to State and local government agencies.

SLP Quarterly Business Activity Reports are due in the SLP Unit within two weeks after the end of each quarter as shown below:

Quarter 1	Jan 1 to Mar 31	Due Apr 15
Quarter 2	Apr 1 to Jun 30	Due Jul 15
Quarter 3	Jul 1 to Sep 30	Due Oct 15
Quarter 4	Oct 1 to Dec 31	Due Jan 15

Each contractor is required to remit to the DGS-PD an incentive fee equal to 1.25% of the total of all local government agency orders (excluding sales tax and freight) placed against their SLP contract(s) for the applicable quarter.

The check covering this fee shall be made payable to the Department of General Services, Software Licensing Program, and be attached to the supporting SLP Quarterly Report.

Mail report and check to:

Department of General Services
Procurement Division, SLP Unit
Quarterly Report Processing
PO Box 989052, MS 2-202
Attn: Software Licensing Program
West Sacramento, CA 95798-9052

SLP Quarterly Reports which include a check made payable to the DGS-SLP Unit must be mailed via hard-copy, and cannot be accepted via facsimile or e-mail.

New contracts for contractors with existing contracts, and extensions or renewals of existing contracts, will be approved ONLY if the contractor has submitted to the SLP Unit all quarterly reports, due. Each quarterly report is required within two weeks of the end of March, June, September, and December of each calendar year. A report is required even when there is no activity.

The report must include the agency name, purchase order number, purchase order date, state agency billing code, pre-tax total order cost, agency contact name, address and phone number, and total dollars for the quarter. Tax must NOT be included in the quarterly report, even if the agency includes tax on the purchase order.

A sample quarterly report indicating required format and information is attached for your reference (Attachment A).

CONTRACTOR INVOICES

Unless otherwise stipulated, the contractor must send their invoices to the department address set forth in the purchase order. Invoices shall be submitted in triplicate and shall include the following:

- Contract number
- Agency purchase order number
- State Agency Bill Code
- Line item number
- Unit price
- Extended line item price
- Invoice total

State sales tax and/or use tax shall be itemized separately and added to each invoice as applicable. The company name on the SLP contract, purchase order and invoice must match or the State Controller's Office will not approve payment.

CONTRACTOR OWNERSHIP INFORMATION

Allied Network Solutions, Inc. is a large business enterprise.

They are also a certified disabled veteran business enterprise, and their OSDS certification #24852 expires on 06/30/2022.

If this certification has expired, the current expiration date for this company's certification should be verified at: CaleProcure (https://caleprocure.ca.gov/pages/index.aspx) or by contacting the Office of Small Business and DVBE Services at (916) 375-4940. Note that some companies have been assigned a new certification number, so use the company name and/or certification number when checking status on-line.

AGENCY NON-COMPLIANCE

Agency non-compliance with the requirements of this contract may result in the loss of delegated purchasing authority to use the SLP.

PLEASE REQUEST A COPY OF ALL CONTRACT TERMS AND CONDITIONS FROM THE CONTRACTOR, IF NOT PROVIDED INITIALLY.

AVAILABLE PRODUCTS AND/OR SERVICES

This contract provides for the purchase and warranty of software, software maintenance, technical support, training, installation, software as a service, infrastructure as a service, platform as a service, and implementation services.

Only products from the manufacturer listed below are available within the scope of this contract:

- **Red Hat**

UNAVAILABLE PRODUCTS AND/OR SERVICES

The following products and/or services are not available under this contract:

- **STANDALONE HARDWARE**

- **CONSULTING**
- **STANDALONE TRAINING**
- **STANDALONE INSTALLATION SERVICES**

Notice to State Agencies: Software appliances/hardware products offered under the Software Publisher's pricelist are NOT available under the Software Licensing Program (SLP) if the same type of software appliance/hardware products are currently available under any mandatory Statewide Contract. State agencies who want to purchase a software appliance/hardware product type, other than what is available through a mandatory Statewide Contract must submit an exemption request to the mandatory Statewide Contract Administrator. For more information and the required justification forms regarding the exemption process, please refer to the following website: https://www.dgs.ca.gov/PD/Services/Page-Content/Procurement-Division-Services-List-Folder/Request-an-IT-Hardware-Contract-Exemption. This restriction does not apply to local governmental agencies.

INSTALLATION SERVICES

- Installation Services can only be purchased when they are in support of software purchased under this SLP contract.
- Installation Services must not exceed the total cost of the software.

IMPLEMENTATION SERVICES

Before procuring Implementation Services, state departments should conduct an analysis and use their own due diligence to determine if these services are the most cost effective solution that meets their business needs and security requirements.

Requirements

- State departments must complete a Statement of Work (SOW) for all Implementation services.
- Job titles/categories are limited to those identified in the SLP price list.
- Hourly rates must not exceed those identified in the SLP price list.
- Implementation services can only be purchased when they are in support of software purchased under the SLP.
- Time and Material pricing must not exceed the job Title hourly rate times the number of hours to complete the job.

NOTE: Implementation Services under this contract must be paid in arrears.

ACQUISITION OF IAAS AND/OR PAAS

If using this SLP for the purpose of acquiring Infrastructure as a Service (IaaS) and/or Platform as a Service (PaaS), State agencies must first obtain approval to use this SLP by the California Department of Technology (CDT) in accordance with TL 17-06 (www.cdt.ca.gov/wp-content/uploads/2017/08/TL-17-06.pdf). State agencies must document CDT's approval and maintain in the procurement file. Contact CDT for all questions related to the acquisition of IaaS and PaaS and TL 17-06.

SOFTWARE MAINTENANCE, SUBSCRIPTION AND SAAS RENEWALS

Software Maintenance, Subscription and SaaS renewals shall be fixed at the agencies prior applicable rates (or lower), with a 0% uplift (no up-lift) and no

additional increases, fees or charges added, for the duration of this SLP

FIRST-YEAR MAINTENANCE

First-year Maintenance for software products are inclusive of subscription.

ISSUE PURCHASE ORDER TO

Agency purchase orders must be mailed to the following address, or e-mail:

Allied Network Solutions, Inc.
5718 Lonetree Boulevard
Rocklin, CA 95765
Attn: Roger Schnorenberg

Agencies with questions regarding products and/or services may contact the contractor as follows:

Phone: (916) 774-2670 Ext. 101
E-mail: rschnorenberg@ans-it.com

SHIPPING INSTRUCTIONS

F.O.B. (Free On Board) Destination

DELIVERY

30 days after receipt of order, or as negotiated between agency and Contractor and included in the purchase order.

AGENCY RESPONSIBILITY

Agencies must contact contractors to obtain copies of the contracts and compare them for a best value purchasing decision.

Each agency is responsible for its own contracting program and purchasing decisions, including use of the SLP program and associated outcomes.

This responsibility includes, but is not necessarily limited to, ensuring the necessity of the services, securing appropriate funding, complying with laws and policies, preparing the purchase order in a manner that safeguards the State's interests, obtaining required approvals, and documenting compliance with Government Code 19130.b (3) for outsourcing services.

It is the responsibility of each agency to consult as applicable with their legal staff and contracting offices for advice depending upon the scope or complexity of the purchase order.

If you do not have legal services available to you within your agency, the DGS Office of Legal Services is available to provide services on a contractual basis.

ORDER REQUIREMENTS AND MAXIMUM ORDER LIMIT

- Unless otherwise determined by an individual ordering agency purchasing authority, no SLP order may be executed by a State agency that exceeds that agency's purchasing authority threshold. State agencies with approved purchasing authority, along with their dollar thresholds can be obtained at the List of State Departments with Approved Purchasing Authority.
- Agencies must adhere to the detailed requirements in the State Contracting Manual (SCM) when using SLP contracts. The requirements for the following bullets are in the SCM, Volume 3, (for IT): If soliciting offers from a certified DVBE, include the Disabled Veteran Business Enterprise Declarations form (Std. 843) in the Request for Offer. This declaration must be completed and returned by the DVBE prime contractor and/or any DVBE subcontractors. (See the SCM Volume 3, Chapter 3)

- This is not a bid transaction, so the small business preference, DVBE participation goals, protest language, intents to award, evaluation criteria, advertising, etc., are not applicable.
- If less than 3 offers are received, State agencies must document their file with the reasons why the other suppliers solicited did not respond with an offer.
- Assess the offers received using best value methodology, with cost as one of the criteria.
- Issue a Purchase Order to the selected contractor.
- For SLP transactions under $10,000, only one offer is required if the State agency can establish and document that the price is fair and reasonable. The fair and reasonable method can only be used for non-customizable purchases.

Local governments set their own order limits, and are not bound by the order limits on the cover page of this contract.

SPLITTING ORDERS

Splitting orders to avoid any monetary limitations is prohibited.

Do not circumvent normal procurement methods by splitting purchases into a series of delegated purchase orders (SAM 3572).

Splitting a project into small projects to avoid either fiscal or procedural controls is prohibited (SAM 4819.34).

MINIMUM ORDER LIMITATION

There is no minimum dollar value limitation on orders placed under this contract.

ORDERING PROCEDURES

1. Order Form

State departments shall use a Contract/Delegation Purchase Order (Std. 65) for purchases and services.

Local governments shall, in lieu of the State's Purchase Order (Std. 65), use their own purchase order document.

Electronic copies of the State Standard Forms can be found at the Office of State Publishing web site: http://www.dgs.ca.gov/osp (select Standard Forms). The site provides information on the various forms and use with the Adobe Acrobat Reader. Beyond the Reader capabilities, Adobe Acrobat advanced features may be utilized if you have Adobe Business Tools or Adobe Acrobat 4.0 installed on your computer. Direct link to the Standard Form 65: (http://www.osp.dgs.ca.gov/pdf/std065.pdf)

2. Purchase Orders

All Ordering Agency purchase order documents executed under this SLP must contain the applicable SLP contract number as show on page 1.

1. State Departments:

   Std. 65 Purchase Documents – State departments not transacting in FI$Cal must use the Purchasing Authority Purchase Order (Std. 65) for purchase execution. An electronic version of the Std. 65 is available at the DGS-PD website at http://www.dgs.ca.gov/pd/Forms.aspx (select Standard STD Forms).

   FI$Cal Purchase Documents – State departments transacting in FI$Cal will follow the FI$Cal

procurement and contracting procedures.

2. Local Governmental Departments:

   Local governmental agencies may use their own purchase document for purchase execution.

The agency is required to complete and distribute the order form. For services, the agency shall modify the information contained on the order to include the service period (start and end date), and the monthly cost (or other intermittent cost), and any other information pertinent to the services being provided. The cost for each line item should be included in the order, not just system totals.

The contractor must immediately reject orders that are not accurate. Discrepancies are to be negotiated and incorporated into the order prior to the products and services being delivered.

3. **Service and Delivery after Contract Expiration**

   Purchase orders must be issued before the SLP contract end term expires.

   Also, purchase order amendments cannot be issued to add product and software maintenance if the SLP contract end term has expired.

CONTRACT PRICES

Contract prices for products and/or services are maximums. The ordering department is encouraged to negotiate lower prices.

PRODUCT AND PRICING CHANGES AND/OR UPDATES ARE NOT AUTHORIZED UNTIL REVIEWED AND APPROVED BY DGS PROCUREMENT DIVISION SOFTWARE LICENSING PROGRAM.

Said documents are to be sent to the Department of General Services (DGS) Procurement Division, Soffware Licensing Program, 707 Third Street, 2nd Floor, West Sacramento, CA 95605-2811, Attention SLP Unit.

CONTRACT EXTENSIONS

The initial term of this SLP contract is 3 years and may be extended for an additional 2-years, however an amendment must be issued prior to contract end date. **NOTE: Extensions are optional and are at the discretion of the state.**

SMALL BUSINESS MUST BE CONSIDERED

Prior to placing orders under the SLP, state departments shall, whenever practicable, first consider offers from small businesses that have established SLP contracts [GC Section 14846(b)]. NOTE: The Department of General Services auditors will request substantiation of compliance with this requirement when department files are reviewed.

SMALL BUSINESS/DVBE – TRACKING

State departments are able to claim subcontracting dollars towards their small business or DVBE goals whenever the Contractor subcontracts a commercially useful function to a certified small business or DVBE. The Contractor will provide the ordering department with the name of the small business or DVBE used and the dollar amount the ordering department can apply towards its small business or DVBE goal.

SMALL BUSINESS/DVBE - SUBCONTRACTING

1. The amount an ordering department can claim towards achieving its small business or DVBE goals is the dollar amount of the subcontract award made by the Contractor to each small business or DVBE.
2. The Contractor will provide an ordering department with the following information at the time the order is quoted:

    a. The Contractor will state that, as the prime Contractor, it shall be responsible for the overall execution of the fulfillment of the order.

    b. The Contractor will indicate to the ordering department how the order meets the small business or DVBE goal, as follows:

    - List the name of each company that is certified by the Office of Small Business and DVBE Certification that it intends to subcontract a commercially useful function to; and
    - Include the small business or DVBE certification number of each company listed, and attach a copy of each certification; and
    - Indicate the dollar amount of each subcontract with a small business or DVBE that may be claimed by the ordering department towards the small business or DVBE goal; and
    - Indicate what commercially useful function the small business or DVBE subcontractor will be providing towards fulfillment of the order.

3. The ordering department's purchase order must be addressed to the prime Contractor, and the purchase order must reference the information provided by the prime Contractor as outlined above.

PRODUCTIVE USE REQUIREMENTS

The customer in-use requirement applies to all procurements of information technology equipment and software, per the SCM, Volume 3, Chapter 2, Section 2.B6.2 and SCM, Volume FI$Cal, Chapter 2, Section 2.E3.2.

Each equipment or software component must be in current operation for a paying customer and the paying customer must be external to the contractor's organization (not owned by the contractor and not owning the contractor).

To substantiate compliance with the Productive Use Requirements, the SLP contractor must provide upon request the name and address of a customer installation and the name and telephone number of a contact person.

The elapsed time such equipment or software must have been in operation is based upon the importance of the equipment or software for system operation and its cost. The following designates product categories and the required period of time for equipment or software operation prior to approval of the replacement item on SLP.

Category 1 - Critical Software: Critical software is software that is required to control the overall operation of a computer system or peripheral equipment. Included in this category are operating systems, data base management systems, language interpreters, assemblers and compilers,

communications software, and other essential system software.

Cost	Installation	Final Bid Submission
More than $100,000	8 months	6 months
$10,000 up to $100,000	4 months	3 months
Less than $10,000	1 month	1 month

Category 2 - All Information Technology Equipment and Non-Critical Software: Information technology equipment is defined in State Administrative Manual (SAM) § 4819.2.

Cost	Installation	Final Bid Submission
More than $100,000	6 months	4 months
$10,000 up to $100,000	4 months	3 months
Less than $10,000	1 month	1 month

STATE AND LOCAL GOVERNMENTS CAN USE THE SLP

State and local government use of the SLP contracts is optional. A local government is any city, county, special district or other local governmental body or corporation, including UC, K-12 schools and community colleges,

that is empowered to expend public funds. While the state makes this contract available, each local government agency should make its own

determination whether the SLP is consistent with their procurement policies and regulations.

APPLICABLE CODES, POLICIES AND GUIDELINES

All California codes, policies and guidelines are applicable. THE USE OF THE SLP DOES NOT REDUCE OR RELIEVE STATE DEPARTMENTS OF THEIR RESPONSIBILITY TO MEET STATEWIDE REQUIREMENTS REGARDING CONTRACTING OR THE PROCUREMENT OF GOODS OR SERVICES. Most procurement and contract codes, policies, and guidelines are incorporated into The SLP contracts. Notwithstanding this, there is no guarantee that "every" possible requirement that pertains to all the different and unique state processes has been included.

TERMINATION OF SLP CONTRACT

1. The State or Contractor may terminate this SLP Contract at any time upon 30 days prior notice.
2. Upon termination or other expiration of this Contract, each party will assist the other party in orderly termination of the Contract and the transfer of all assets, tangible and intangible, as may facilitate the orderly, nondisrupted business continuation of each party.
3. This provision shall not relieve the Contractor of the obligation to perform under any purchase order or other similar ordering document executed prior to the termination becoming effective.

STATEWIDE PROCUREMENT REQUIREMENTS

Departments must carefully review and adhere to the following Procurement Requirements, such as:

- SAM Section 4819.41 and 4832 certifications for information technology

procurements and compliance with policies.

- Services may not be paid for in advance.
- Departments are required to file with the Department of Fair Employment and Housing (DFEH) a Contract Award Report Std. 16 for each order over $5,000 within 10 days of award, including supplements that exceed $5,000.
- Pursuant to Unemployment Insurance Code Section 1088.8, state and local government agencies must report to the Employment Development Department (EDD) all payments for services that equal $600 or more to independent sole proprietor contractors. See the contractor's Std. Form 204, Payee Data Record, in the SLP contract to determine sole proprietorship. All inquiries regarding this subject should be forwarded to EDD: Technical questions: 916/651-6945 or Information and forms: 916/657-0529.
- Annual small business and disabled veteran reports.

ETHNICITY/RACE/GENDER REPORTING REQUIREMENT

Effective July 1, 2002, in accordance with Public Contract Code 10116, state departments are to capture information on ethnicity, race, and gender of business owners (not subcontractors) for all awarded contracts, including CAL-Card transactions. Each department is required to independently report this information to the Governor and the Legislature on an annual basis.

Departments are responsible for developing their own guidelines and forms for collecting and reporting this information.

Contractor participation is voluntary.

PAYMENTS AND INVOICES

1. Payment Terms

Payment will be made in accordance with the provisions of the California Prompt Payment Act, Government Code Section 927 et. seq. Unless expressly exempted by statute, the Act requires State agencies to pay properly submitted, undisputed invoices not more than 45 days after (i) the date of acceptance of goods or performance of services; or (ii) receipt of an undisputed invoice, whichever is later.

2. Advance Payments

Advance payment is allowed for services only under limited, narrowly defined circumstances, e.g. between specific departments and certain types of non-profit organizations, or when paying another government agency (Government Code (GC) § 11256 – 11263 and 11019).

It is NOT acceptable to pay in advance, except software maintenance and license fees, which are considered a subscription and may be paid in advance if a provision addressing payment in advance is included in the purchase order.

Software warranty upgrades and extensions may also be paid for in advance, one time.

3. Payee Data Record (Std. 204)

State Agencies not transacting in FI$Cal, must obtain a copy of the Payee Data Record (Std. 204) in order to process payments. State Ordering Agencies forward a copy of

the Std. 204 to their accounting office(s). Without the Std. 204, payment may be unnecessarily delayed. State Agencies should contact the Contractor for copies of the Payee Data Record

4. **DGS Administrative and Incentive Fees**

Orders from State Agencies:

The Department of General Services (DGS) will bill each State agency directly an administrative fee for use of SLP contracts. The administrative fee should NOT be included in the order total, nor remitted before an invoice is received from DGS.

5. **Credit Card**

Allied Network Solutions, Inc. accepts the State of California credit card (CAL-Card).

A Purchasing Authority Purchase Order (Std. 65) is required even when the ordering department chooses to pay the contractor via the CAL-Card. Also, the DGS administrative fee is applicable for all SLP orders to suppliers not California certified as a small business.

FEDERAL DEBARMENT

When federal funds are being expended, the department is required to obtain (retain in file) a signed "Federal Debarment" certification from the contractor before the purchase order is issued. This certification is required 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).

AMERICANS WITH DISABILITY ACT (ADA)

(See attachment B)

DGS PROCUREMENT DIVISION CONTACT AND PHONE NUMBER

Department of General Services
Procurement Division, SLP Unit
707 Third Street, 2nd Floor
West Sacramento, CA 95605-2811

Phone no.: **916/375-4365**
Faxination no.: **916/376-6371**

ATTACHMENT A

SLP QUARTERLY BUSINESS ACTIVITY REPORT

Company Name: _____

Software Publisher: _____

Contract Number: _____

For Questions Regarding this Report: _____

E-mail: _____

Reporting Calendar Year: _____

Reporting Quarter:
- ☐ Q1 (January to March)
- ☐ Q2 (April to June)
- ☐ Q3 (July to September)
- ☐ Q4 (October to December)

Check Here if No New Orders for This Quarter ☐

STATE GOVERNMENT AGENCY PURCHASES

State Agency Name	Purchase Order Number	Purchase Order Date	Agency Billing Code	Total Dollars Per Purchase Order	Agency Contact	Agency Address	Phone Number

Total State Agency Dollars Reported for Quarter: $_____

LOCAL GOVERNMENT AGENCY PURCHASES

Local Government Agency Name	Purchase Order Number	Purchase Order Date	Total Dollars Per Purchase Order	Agency Contact	Agency Address	Phone Number

Total Local Government Agency Dollars for Quarter: $_____

1.25% Remitted to DGS (does not apply to CA certified Small Businesses): $ _____

Total of State and Local Government Agency Dollars Reported for this Quarter: $_____

ATTACHMENT A

SLP QUARTERLY BUSINESS ACTIVITY REPORT

Instructions for completing the SLP Quarterly Business Activity Report.

1. Complete the top of the form with the appropriate information for your company.
2. **Agency Name** - Identify the State agency or Local Government agency that issued the order.
3. **Purchase Order Number** - Identify the purchase order number (and amendment number if applicable) on the order form. This is not your invoice number. This is the number the State agency or Local Government agency assigns to the order.
4. **Purchase Order Date** - Identify the date the purchase order was issued, as shown on the order. This is not the date you received, accepted, or invoiced the order.
5. **Agency Billing Code** - Identify the State agency billing code. This is a five-digit number identified on the upper right hand corner of the Std. 65 purchase order form. You must identify this number on all purchases made by State of California agencies. Billing codes are not applicable to Local Government agencies.
6. **Total Dollars Per PO** - Identify the total dollars of the order excluding tax and freight. Tax must NOT be included in the quarterly report, even if the agency includes tax on the purchase order. The total dollars per order should indicate the entire purchase order amount (less tax and freight) regardless of when you invoice order, perform services, deliver product, or receive payment.
7. **Agency Contact** - Identify the ordering agency's contact person on the purchase order.
8. **Agency Address** - Identify the ordering agency's address on the purchase order.
9. **Phone Number** - Identify the phone number for the ordering agency's contact person.
10. **Total State Sales & Total Local Sales** - Separately identify the total State dollars and/or Local Government agency dollars (pre-tax) for all orders placed in quarter.
11. **1.25% Remitted to DGS** - Identify 1.25% of the total Local Government agency dollars reported for the quarter.
12. **Grand Total** - Identify the total of all State and Local Government agency dollars reported for the quarter.

Notes:

- A report is required for each SLP contract each quarter even when there are no new orders for the quarter.
- Quarterly reports are due two weeks after the end of the quarter.

ATTACHMENT B

ADA NOTICE

Procurement Division (State Department of General Services)
AMERICANS WITH DISABILITIES ACT (ADA) COMPLIANCE
POLICY OF NONDISCRIMINATION ON THE BASIS OF DISABILITY

To meet and carry out compliance with the nondiscrimination requirements of the Americans With Disabilities Act (ADA), it is the policy of the Procurement Division (within the State Department of General Services) to make every effort to ensure that its programs, activities, and services are available to all persons, including persons with disabilities.

For persons with a disability needing a reasonable accommodation to participate in the Procurement process, or for persons having questions regarding reasonable accommodations for the Procurement process, please contact the Procurement Division at (916) 375-4400 (main office); the Procurement Division TTY/TDD (telephone device for the deaf) or California Relay Service numbers which are listed below. You may also contact directly the Procurement Division contact person who is handling this procurement.

IMPORTANT: TO ENSURE THAT WE CAN MEET YOUR NEED, IT IS BEST THAT WE RECEIVE YOUR REQUEST AT LEAST 10 WORKING DAYS BEFORE THE SCHEDULED EVENT (i.e., MEETING, CONFERENCE, WORKSHOP, etc.) OR DEADLINE DUE-DATE FOR PROCUREMENT DOCUMENTS.

The Procurement Division TTY telephone numbers are:

Sacramento Office:	(916) 376-1891
Fullerton Office:	(714) 773-2093

The California Relay Service Telephone Numbers are:

Voice:	1-800-735-2922 or 1-888-877-5379
TTY:	1-800-735-2929 or 1-888-877-5378
Speech-to-Speech:	1-800-854-7784

CALIFORNIA DEPARTMENT OF GENERAL SERVICES

Procurement Division
707 Third Street, 2nd Floor, MS #2-202
West Sacramento, CA 95605-2811

State of California
SOFTWARE LICENSING PROGRAM (SLP)
AMENDMENT NO. 1

softwarelicensingprogram

Contractor:	Allied Network Solutions, Inc.
Contract Number:	SLP-22-70-0027O
SLP Contract Term:	1/1/2022 through 12/31/2025
Contract Base:	Red Hat Offer Number RedHat-SLP-2022

This amendment is being issued to:

Add the provision **"GENERATIVE ARTIFICIAL INTELLIGENCE (GENAI) REPORTING"**

GENERATIVE ARTIFICIAL INTELLIGENCE (GENAI) REPORTING

1. State Agencies

State agencies are required to obtain a GenAI Reporting and Factsheet (STD 1000) from the Contractor prior to award.

If GenAI is disclosed by the Contractor, state agencies must follow the required GenAI purchase procedures outlined in State Contracting Manual (SCM) Volume 2, Chapter 23, Generative Artificial Intelligence (GenAI). State agencies must retain the STD 1000 and confirmation the purchase may proceed in their procurement file.

2. Contractor

Upon request by an ordering agency, Contractor must complete a GenAI Reporting and Fact Sheet (STD 1000) to identify if their solution or service includes, or makes available, any GenAI including, GenAI from third parties or subcontractors.

During the term of the contract, Contractor must notify the State in writing if their services or any work under this contract includes, or makes available, any previously unreported GenAI technology, including GenAI from third parties or subcontractors. Contractor shall immediately complete the GenAI Reporting and Factsheet (STD 1000) to notify the State of any new or previously unreported GenAI technology.

At the direction of the State, Contractor shall discontinue the use of any new or previously undisclosed GenAI technology that materially impacts functionality, risk or contract performance, until use of such GenAI technology has been approved by the State.

Failure to disclose GenAI use to the State and submit the GenAI Reporting and Factsheet (STD 1000) may be considered a breach of the contract by the State at its sole discretion and the State may consider such failure to disclose GenAI and/or failure to submit the GenAI Reporting and Factsheet (STD 1000) as grounds for the immediate termination of the contract. The State is entitled to seek any and all relief to which it may be entitled to as a result of such non-disclosure.

SOFTWARE LICENSING PROGRAM (SLP)
ALLIED NETWORK SOLUTIONS, INC.
SLP-22-70-0027O AMENDMENT NO. 1

The State reserves the right to amend the contract, without additional cost, to incorporate GenAI Special Provisions into the contract at its sole discretion and/or terminate any contract that presents an unacceptable level of risk to the State.

If Contractor identifies GenAI in their solution, a copy of the STD 1000 must be submitted to the State Contract Administrator.

ALL OTHER TERMS AND CONDITIONS REMAIN THE SAME.

For State of CA:

Original Signature on File

Stephanne Lim
Manager
Multiple Award Programs Section
Procurement Division
Department of General Services

10/22/2024
Date

For Contractor:

Original Signature on File

Signature

Printed Title

Printed Name

Company Name

Date

STATE MODEL
CLOUD COMPUTING SERVICES SPECIAL PROVISIONS
(Software as a Service)

THESE SPECIAL PROVISIONS ARE ONLY TO BE USED FOR SOFTWARE AS A SERVICE (SaaS), AS DEFINED BELOW. THESE SPECIAL PROVISIONS ARE TO BE ATTACHED TO THE GENERAL PROVISIONS – INFORMATION TECHNOLOGY AND SHOULD BE ACCOMPANIED BY, A STATEMENT OF WORK (SOW) AND SERVICE LEVEL AGREEMENT (SLA). SECURITY REQUIREMENTS DESIGNATED IN THIS DOCUMENT ARE ASSUMING A NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST) LOW CLASSIFICATION, UNLESS OTHERWISE SET FORTH IN THE SOW. A HIGHER CLASSIFICATION MAY REQUIRE DIFFERENT SECURITY REQUIREMENTS. STATE AGENCIES MUST FIRST:

A. **CLASSIFY THEIR DATA PURSUANT TO THE CALIFORNIA STATE ADMINISTRATIVE MANUAL (SAM) 5305.5;**
B. **CONSIDER THE FACTORS TO BE TAKEN INTO ACCOUNT WHEN SELECTING A PARTICULAR TECHNOLOGICAL APPROACH, IN ACCORDANCE WITH SAM 4981.1, 4983 AND 4983.1 AND THEN;**
C. **MODIFY THESE SPECIAL PROVISIONS THROUGH THE SOW AND/OR SLA TO MEET THE NEEDS OF EACH ACQUISITION.**

1. Definitions

a) "**Cloud Software as a Service (SaaS)**" - The capability provided to the consumer is to use applications made available by the provider running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a web browser (e.g., web-based email). The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

b) "**Cloud Platform as a Service (PaaS)**" - The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.

c) "**Cloud Infrastructure as a Service (IaaS)**" - The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems; storage, deployed applications, and possibly limited control of select networking components (e.g., host firewalls).

d) "**Data**" - means any information, formulae, algorithms, or other content that the State, the State's employees, agents and end users upload, create or modify using the SaaS pursuant to this Contract. Data also includes user identification information and metadata which may contain Data or from which the State's Data may be ascertainable.

e) "**Data Breach**" - means any access, destruction, loss, theft, use, modification or disclosure of Data by an unauthorized party or that is in violation of Contract terms and/or applicable state or federal law.

f) "**Encryption**" - Conversion of plaintext to ciphertext through the use of a Federal Information Processing Standards (FIPS) validated cryptographic algorithm. [FIPS 140-2]

g) "**Recovery Point Objective (RPO)**" - means the point in time to which Data can be recovered and/or systems restored when service is restored after an interruption. The Recovery Point Objective is expressed as a length of time between the interruption and the most proximate backup of Data immediately preceding the interruption. The RPO is detailed in the SLA.

h) "**Recovery Time Objective (RTO)**" - means the period of time within which information technology services, systems, applications and functions must be recovered following an unplanned interruption. The RTO is detailed in the SLA.

Terms

2. SaaS AVAILABILITY: Unless otherwise stated in the Statement of Work,

a) The SaaS shall be available twenty-four (24) hours per day, 365 days per year (excluding agreed-upon maintenance downtime).
b) If SaaS monthly availability averages less than 99.9% (excluding agreed-upon maintenance downtime), the State shall be entitled to recover damages, apply credits or use other contractual remedies as set forth in the Statement of Work.
c) If SaaS monthly availability averages less than 99.9% (excluding agreed-upon maintenance downtime), for three (3) or more months in a rolling twelve-month period, the State may terminate the contract for material breach in accordance with the Termination for Default provision in the General Provisions – Information Technology.
d) Contractor shall provide advance written notice to the State in the manner set forth in the Statement of Work of any major upgrades or changes that will affect the SaaS availability.

3. DATA AVAILABILITY: Unless otherwise stated in the Statement of Work,

a) The Data shall be available twenty-four (24) hours per day, 365 days per year (excluding agreed-upon maintenance downtime).
b) If Data monthly availability averages less than 99.9% (excluding agreed-upon maintenance downtime), the State shall be entitled to recover damages, apply credits or use other contractual remedies as set forth in the Statement of Work if the State is unable to access the Data as a result of:
    1) Acts or omission of Contractor;
    2) Acts or omissions of third parties working on behalf of Contractor;
    3) Network compromise, network intrusion, hacks, introduction of viruses, disabling devices, malware and other forms of attack that can disrupt access to Contractor's server, to the extent such attack would have been prevented by Contractor taking reasonable industry standard precautions;
    4) Power outages or other telecommunications or Internet failures, to the extent such outages were within Contractor's direct or express control.
c) If Data monthly availability averages less than 99.9% (excluding agreed-upon maintenance downtime), for three (3) or more months in a rolling twelve-month period, the State may terminate the contract for material breach in accordance with the Termination for Default provision in the General Provisions – Information Technology.

4. SaaS and DATA SECURITY:

a) In addition to the Compliance with Statutes and Regulations provision set forth in the General Provisions – Information Technology, Contractor shall certify to the State:
    1) The sufficiency of its security standards, tools, technologies and procedures in providing SaaS under this Contract;
    2) Compliance with the following:
        i. The California Information Practices Act (Civil Code Sections 1798 et seq.);
        ii. Current NIST special publications 800-171 Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations. Third party audit results and Contractor's plan to correct any negative findings shall be made available to the State upon request ;

iii. Undergo an annual Statement on Standards for Attestation Engagements (SSAE) No. 16 Service Organization Control (SOC) 2 Type II audit. Third party audit results and Contractor's plan to correct any negative findings and implementation progress reports shall be made available to the State upon request; and
iv. Privacy provisions of the Federal Privacy Act of 1974;

3) Compliance with industry standards and guidelines applicable to the SaaS services being provided. Relevant security provisions may include, but are not limited to: Health Insurance Portability and Accountability Act of 1996, IRS 1075, Health Information Technology for Economic and Clinical (HITECH) Act, Criminal Justice Information Services (CJIS) Security Policy, Social Security Administration (SSA) Electronic Information Exchange Security Requirements, and the Payment Card Industry (PCI) Data Security Standard (DSS) as well as their associated Cloud Computing Guidelines.

b) Contractor shall implement and maintain all appropriate administrative, physical, technical and procedural safeguards in accordance with section a) above at all times during the term of this Contract to secure such Data from Data Breach, protect the Data and the SaaS from hacks, introduction of viruses, disabling devices, malware and other forms of malicious or inadvertent acts that can disrupt the State's access to its Data.
c) Contractor shall allow the State reasonable access to SaaS security logs, latency statistics, and other related SaaS security data that affect this Contract and the State's Data, at no cost to the State.
d) Contractor assumes responsibility for the security and confidentiality of the Data under its control.
e) No Data shall be copied, modified, destroyed or deleted by Contractor other than for normal operation or maintenance of SaaS during the Contract period without prior written notice to and written approval by the State.
f) Remote access to Data from outside the continental United States, including remote access to Data by authorized SaaS support staff in identified support centers, is prohibited unless approved in advance in writing by:
    1) the Agency Information Security Officer, with written notice to the State Chief Information Security Officer, or
    2) in the absence of an Agency Information Security Officer, the State Chief Information Security Officer.

5. ENCRYPTION: Confidential, sensitive or personal information shall be encrypted in accordance with California State Administrative Manual 5350.1 and California Statewide Information Management Manual 5305-A.

6. DATA LOCATION: Unless otherwise stated in the Statement of Work and approved in advance in writing by:
1) the Agency Information Security Officer, with written notice to the State Chief Information Security Officer, or
2) in the absence of an Agency Information Security Officer, the State Chief Information Security Officer,

the physical location of Contractor's data center where the Data is stored shall be within the continental United States.

7. RIGHTS TO DATA: The parties agree that as between them, all rights, including all intellectual property rights, in and to Data shall remain the exclusive property of the State, and Contractor has a limited, non-exclusive license to access and use the Data as provided to Contractor solely for performing its obligations under the Contract. Nothing herein shall be construed to confer any license or right to the Data, including user tracking and exception Data within the system, by implication, estoppel or otherwise, under copyright or other intellectual property rights, to any third party. Unauthorized use of Data by Contractor or third parties is prohibited. For the purposes of this requirement,

the phrase "unauthorized use" means the data mining or processing of data, stored or transmitted by the service, for unrelated commercial purposes, advertising or advertising-related purposes, or for any other purpose other than security or service delivery analysis that is not explicitly authorized.

8. TRANSITION PERIOD:

a) Unless otherwise stated in the SOW, for ninety (90) days prior to the expiration date of this Contract, or upon notice of termination of this Contract, Contractor shall assist the State in extracting and/or transitioning all Data in the format determined by the State ("Transition Period").
b) The Transition Period may be modified in the SOW or as agreed upon in writing by the parties in a contract amendment.
c) During the Transition Period, SaaS and Data access shall continue to be made available to the State without alteration.
d) Contractor agrees to compensate the State for damages or losses the State incurs as a result of Contractor's failure to comply with this section in accordance with the Limitation of Liability provision set forth in the General Provisions - Information Technology.
e) Unless otherwise stated in the SOW, the Contractor shall permanently destroy or render inaccessible any portion of the Data in Contractor's and/or subcontractor's possession or control following the expiration of all obligations in this section. Within thirty (30) days, Contractor shall issue a written statement to the State confirming the destruction or inaccessibility of the State's Data.
f) The State at its option, may purchase additional transition services as agreed upon in the SOW.

9. DATA BREACH: Unless otherwise stated in the Statement of Work,

a) Upon discovery or reasonable belief of any Data Breach, Contractor shall notify the State by the fastest means available and also in writing, with additional notification provided to the Chief Information Security Officer or designee of the contracting agency. Contractor shall provide such notification within forty-eight (48) hours after Contractor reasonably believes there has been such a Data Breach. Contractor's notification shall identify:
    1) The nature of the Data Breach;
    2) The Data accessed, used or disclosed;
    3) The person(s) who accessed, used, disclosed and/or received Data (if known);
    4) What Contractor has done or will do to quarantine and mitigate the Data Breach; and
    5) What corrective action Contractor has taken or will take to prevent future Data Breaches.
b) Contractor will provide daily updates, or more frequently if required by the State, regarding findings and actions performed by Contractor until the Data Breach has been effectively resolved to the State's satisfaction.
c) Contractor shall quarantine the Data Breach, ensure secure access to Data, and repair SaaS as needed in accordance with the SLA. Failure to do so may result in the State exercising its options for assessing damages or other remedies under this Contract.
d) Notwithstanding anything to the contrary in the General Provisions - Information Technology, in performing services under this Contract, and to the extent authorized by the State in the Statement of Work, Contractor may be permitted by the State to use systems, or may be granted access to the State systems, which store, transmit or process State owned, licensed or maintained computerized Data consisting of personal information, as defined by Civil Code Section 1798.29 (g). If the Contractor causes or knowingly experiences a breach of the security of such Data, Contractor shall immediately report any breach of security of such system to the State following discovery or notification of the breach in the security of such Data. The State's Chief Information Security Officer, or designee, shall determine whether notification to the individuals whose Data has been lost or breached is appropriate. If personal information of any resident of California was, or is reasonably believed to have been acquired by an unauthorized person as a result of a

security breach of such system and Data that is not due to the fault of the State or any person or entity under the control of the State, Contractor shall bear any and all costs associated with the State's notification obligations and other obligations set forth in Civil Code Section 1798.29 (d) as well as the cost of credit monitoring, subject to the dollar limitation, if any, agreed to by the State and Contractor in the applicable Statement of Work. These costs may include, but are not limited to staff time, material costs, postage, media announcements, and other identifiable costs associated with the breach of the security of such personal information.

e) Contractor shall conduct an investigation of the Data Breach and shall share the report of the investigation with the State. The State and/or its authorized agents shall have the right to lead (if required by law) or participate in the investigation. Contractor shall cooperate fully with the State, its agents and law enforcement.

10. DISASTER RECOVERY/BUSINESS CONTINUITY: Unless otherwise stated in the Statement of Work,

a) In the event of disaster or catastrophic failure that results in significant Data loss or extended loss of access to Data, Contractor shall notify the State by the fastest means available and also in writing, with additional notification provided to the Chief Information Security Officer or designee of the contracting agency. Contractor shall provide such notification within twenty-four (24) hours after Contractor reasonably believes there has been such a disaster or catastrophic failure. In the notification, Contactor shall inform the State of:
    1) The scale and quantity of the Data loss;
    2) What Contractor has done or will do to recover the Data and mitigate any deleterious effect of the Data loss; and
    3) What corrective action Contractor has taken or will take to prevent future Data loss.
    4) If Contractor fails to respond immediately and remedy the failure, the State may exercise its options for assessing damages or other remedies under this Contract.

b) Contractor shall restore continuity of SaaS, restore Data in accordance with the RPO and RTO as set forth in the SLA, restore accessibility of Data, and repair SaaS as needed to meet the performance requirements stated in the SLA. Failure to do so may result in the State exercising its options for assessing damages or other remedies under this Contract.

c) Contractor shall conduct an investigation of the disaster or catastrophic failure and shall share the report of the investigation with the State. The State and/or its authorized agents shall have the right to lead (if required by law) or participate in the investigation. Contractor shall cooperate fully with the State, its agents and law enforcement.

11. EXAMINATION AND AUDIT: In addition to the Examination and Audit provision set forth in the General Provisions - Information Technology, unless otherwise stated in the Statement of Work:

a) Upon advance written request, Contractor agrees that the State or its designated representative shall have access to Contractor's SaaS, operational documentation, records and databases, including online inspections, that relate to the SaaS purchased by the State.

b) The online inspection shall allow the State, its authorized agents, or a mutually acceptable third party to test that controls are in place and working as intended. Tests may include, but not be limited to, the following:
    1) Operating system/network vulnerability scans,
    2) Web application vulnerability scans,
    3) Database application vulnerability scans, and
    4) Any other scans to be performed by the State or representatives on behalf of the State.

c) After any significant Data loss or Data Breach or as a result of any disaster or catastrophic failure, Contractor will at its expense have an independent, industry-recognized, State-approved third party perform an information security audit. The audit results shall be shared with the State within seven (7) days of Contractor's receipt of such results. Upon Contractor receiving the results of the audit, Contractor will

provide the State with written evidence of planned remediation within thirty (30) days and promptly modify its security measures in order to meet its obligations under this Contract.

12. DISCOVERY: Contractor shall promptly notify the State upon receipt of any requests which in any way might reasonably require access to the Data of the State or the State's use of the SaaS. Contractor shall notify the State by the fastest means available and also in writing, with additional notification provided to the Chief Information Security Officer or designee of the contracting agency, unless prohibited by law from providing such notification. Contractor shall provide such notification within forty-eight (48) hours after Contractor receives the request. Contractor shall not respond to subpoenas, service of process, Public Records Act requests, and other legal requests directed at Contractor regarding this Contract without first notifying the State unless prohibited by law from providing such notification. Contractor agrees to provide its intended responses to the State with adequate time for the State to review, revise and, if necessary, seek a protective order in a court of competent jurisdiction. Contractor shall not respond to legal requests directed at the State unless authorized in writing to do so by the State.

STATE MODEL
CLOUD COMPUTING SERVICES SPECIAL PROVISIONS
(Infrastructure as a Service and Platform as a Service)

THESE SPECIAL PROVISIONS ARE ONLY TO BE USED FOR INFRASTRUCTURE AS A SERVICE (IaaS) AND PLATFORM AS A SERVICE (PaaS), AS DEFINED BELOW. THESE SPECIAL PROVISIONS ARE TO BE ATTACHED TO THE GENERAL PROVISIONS – INFORMATION TECHNOLOGY AND ACCOMPANIED BY, AT MINIMUM, A STATEMENT OF WORK (SOW) AND SERVICE LEVEL AGREEMENT (SLA). STATE AGENCIES MUST FIRST:

A: CLASSIFY THEIR DATA PURSUANT TO THE CALIFORNIA STATE ADMINISTRATIVE MANUAL (SAM) 5305.5;
B: CONSIDER THE FACTORS TO BE TAKEN INTO ACCOUNT WHEN SELECTING A PARTICULAR TECHNOLOGICAL APPROACH, IN ACCORDANCE WITH SAM 4981.1, 4983 AND 4983.1 AND THEN;
C: MODIFY THESE SPECIAL PROVISIONS THROUGH THE SOW AND/OR SLA TO MEET THE NEEDS OF EACH ACQUISITION.

1. DEFINITIONS:

A. "Authorized Persons" means the Service Provider's employees, Contractors, subcontractors or other agents who need to access the State's Data to enable the Service Provider to perform the services required.

B. "Data Breach" means the unauthorized access that results in the use, disclosure, destruction, modification, loss or theft of the State's unencrypted Personal Data or Non-Public Data.

C. "Individually Identifiable Health Information" means Information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

D. "Infrastructure-as-a-Service" (IaaS) means the capability provided to the consumer is to provision processing, storage, networks and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed application; and possibly limited control of select networking components (e.g., host firewalls).

E. "Non-Public Data" means data submitted to the Service Provider's IaaS or PaaS Service, other than Personal Data, that is not subject to distribution to the public as public information. It is deemed to be sensitive and confidential by the State because it contains information that is exempt by statute, regulation or policy from access by the general public as public information.

F. "Personal Data" means data submitted to the Service Provider's IaaS or PaaS Service that includes information relating to a person that identifies the person by name and has any of the following personally identifiable information (PII): government-issued identification numbers (e.g., Social Security, driver's license, passport); financial account information, including account number, credit or debit card numbers; or protected health information (PHI) relating to a person.

G. "Platform-as-a-Service" (PaaS) means the capability provided to the consumer to deploy onto the cloud infrastructure consumer- created or -acquired applications created using programming languages and tools supported by the provider. This capability does not necessarily preclude the use of compatible programming languages, libraries, services and tools from other sources. The consumer does not manage or control the underlying cloud infrastructure, including network, servers, operating systems or storage, but has control over the deployed applications and possibly application hosting environment configurations.

H. "Protected Health Information" (PHI) means Individually Identifiable Health Information transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA) as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer.

I. "Security Incident" means the potentially unauthorized access to Personal Data or Non-Public Data the Service Provider believes could reasonably result in the use, disclosure or theft of the State's unencrypted Personal Data or Non-Public Data within the possession or control of the Service Provider. A Security Incident may or may not turn into a Data Breach.

J. "Service Level Agreement" (SLA) means a written agreement between both the State and the Service Provider that is subject to the terms and conditions in this document that unless otherwise agreed to includes (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, (4) security responsibilities and notice requirements, how disputes are discovered and addressed, and (6) any remedies for performance failures.

K. "Service Provider" means the Contractor, subcontractors, agents, resellers, third parties and affiliates who are providing the services agreed to under the Contract.

L. "State Data" means all data created or in any way originating with the State, and all data that is the output of computer processing of or other electronic manipulation of any data that was created by or in any way originated with the State, whether such data or output is stored on the State's hardware, the Service Provider's hardware or exists in any system owned, maintained or otherwise controlled by the State or by the Service Provider.

M. "State Identified Contact" means the person or persons designated in writing by the State to receive Security Incident or Data Breach notification.

N. "Statement of Work" (SOW) means a written statement in a Contract that describes the State's service needs and expectations.

2. DATA OWNERSHIP:

The State will own all right, title and interest in State Data that is related to the services provided by this Contract. The Service Provider shall not access State user accounts or State Data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this Contract, (4) at the State's written request or (5) as required by law.

3. DATA PROTECTION:

Protection of personal privacy and data shall be an integral part of the business activities of the Service Provider to ensure there is no inappropriate or unauthorized use of State information at any time. To this end, the Service Provider shall safeguard the confidentiality, integrity and availability of State information within its control and comply with the following conditions:

A. In addition to the Compliance with Statues and Regulations provisions set forth in the General Provisions – Information Technology, the Service Provider shall comply as required with:

   i. The California Information Practices Act (Civil Code Sections 1798 et seq).
   ii. NIST Special Publication 800-53 Revision 4 or its successor.
   iii. Privacy provisions of the Federal Privacy Act of 1974.

B. All State Data obtained by the Service Provider within its control in the performance of this Contract shall become and remain the property of the State.

C. Unless otherwise set forth in the SOW and/or SLA, Personal Data and Non-Public Data shall be encrypted at rest, in use, and in transit with controlled access. The SOW and/or SLA will specify which party is responsible for encryption and access control of the State Data for the service model under Contract. If the SOW and/or SLA and the Contract are silent, then the State is responsible for encryption and access control.

D. Unless otherwise set forth in the SOW and/or SLA, it is the State's responsibility to identify data it deems as Non-Public Data to the Service Provider. The level of protection and encryption for all Non-Public Data shall be identified and made a part of this Contract.

E. At no time shall any Personal Data and Non-Public Data or processes — which either belong to or are intended for the use of State or its officers, agents or employees — be copied, disclosed or retained by the Service Provider or any party related to the Service Provider for subsequent use in any transaction without the express written consent of the State except as permitted in Section 2 above.

F. **(For PaaS Only)** Encryption of Data at Rest: The Service Provider shall ensure hard drive encryption consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data and Non-Public Data, unless the Service Provider presents a justifiable position approved by the State that Personal Data and Non-Public Data must be stored on a Service Provider portable device in order to accomplish work as defined in the SOW and/or SLA.

4. DATA LOCATION:

The Service Provider shall provide its services to the State and its end users solely from data centers in the continental United States. Storage of State Data at rest shall be located solely in data centers in the continental United States. The Service Provider shall not allow its personnel or contractors to store State Data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Service Provider shall permit its personnel and contractors to access State Data remotely only as required to provide technical user support or other customer support. The Service Provider may provide technical user support or other customer support on a 24/7 basis using a Follow the Sun model, unless otherwise prohibited in this Contract.

5. SECURITY INCIDENT OR DATA BREACH NOTIFICATION:

The Service Provider shall inform the State of any Security Incident or Data Breach related to State Data within the possession or control of the Service Provider and related to the service provided under this Contract.

A. Security Incident Reporting Requirements: Unless otherwise set forth in the SOW and/or SLA, the Service Provider shall promptly report a Security Incident related to its service under the Contract to the appropriate State Identified Contact as defined in the SOW and/or SLA.

B. Breach Reporting Requirements: If the Service Provider has actual knowledge of a confirmed Data Breach that affects the security of any State Data that is subject to applicable Data Breach notification law, the Service Provider shall (1) promptly notify the appropriate State Identified Contact within 24 hours or sooner, unless otherwise required by applicable law, and (2) take commercially reasonable measures to address the Data Breach in a timely manner.

C. **(For PaaS Only)** Incident Response: The Service Provider may need to communicate with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing Security Incidents with the State should be handled on an urgent as- needed basis, as part of Service Provider communication and mitigation processes as mutually agreed, defined by law or contained in the Contract.

6. DATA BREACH RESPONSIBILITIES:

This section only applies when a Data Breach occurs with respect to Personal Data and/or Non-Public Data within the possession or control of a Service Provider and related to service provided under this Contract.

A. The Service Provider, unless otherwise set forth in in the SOW and/or SLA, shall promptly notify the appropriate State Identified Contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it confirms that there is or reasonably believes that there has been a Data Breach. The Service Provider shall (1) cooperate with the State as reasonably requested by the State to investigate and resolve the Data Breach; (2) promptly implement necessary remedial measures, if necessary; and (3) document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

B. Service Provider will provide daily updates, or more frequently if required by the State, regarding findings and actions performed by Service Provider to the State Identified Contact until the Data Breach has been effectively resolved to the State's satisfaction.

C. Service Provider shall quarantine the Data Breach, ensure secure access to Data, and repair IaaS and/or PaaS as needed in accordance with the SOW and/or SLA. Failure to do so may result in the State exercising its options for assessing damages or other remedies under this Contract.

D. Unless otherwise set forth in the SOW and/or SLA, if a Data Breach is a direct result of the Service Provider's breach of its Contract obligation to encrypt Personal Data and/or Non-Public Data or otherwise prevent its release, the Service Provider shall bear the costs associated with (1) the investigation and resolution of the Data Breach; (2) notifications to individuals, regulators or others required by State law; (3) a credit monitoring service required by State (or Federal) law; (4) a website or a toll-free number and call center for affected individuals required by State law; and (5) complete all corrective actions as reasonably determined by the Service Provider based on root cause; all [(1) through (5)] subject to this Contract's Limitation of Liability provision as set forth in the General Provisions – Information Technology.

7. NOTIFICATION OF LEGAL REQUESTS:

Unless otherwise required by law, the Service Provider shall contact the State upon receipt of any electronic discovery, litigation holds, discovery searches and expert testimonies related to the State's Data under this Contract, or which in any way might reasonably require access to State's Data. The Service Provider shall not respond to subpoenas, service of process and other legal requests related to the State without first notifying the State, unless prohibited by law from providing such notice. Unless otherwise required by law, Service Provider agrees to provide its intended responses to the State with adequate time for the State to review, revise and, if necessary, seek a protective order in a court of competent jurisdiction. Service Provider shall not respond to legal requests directed at the State unless authorized in writing to do so by the State.

8. DATA PRESERVATION AND RETRIEVAL:

A. For ninety (90) days prior to the expiration date of this Contract, or upon notice of termination of this Contract, Service Provider shall assist the State in extracting and/or transitioning all State Data in the format determined by the State ("Transition Period").

B. The Transition Period may be modified in the SOW and/or SLA or as agreed upon in writing by the parties in a Contract amendment.

C. During the Transition Period, IaaS and/or PaaS and State Data access shall continue to be made available to the State without alteration.

D. Service Provider agrees to compensate the State for damages or losses the State incurs as a result of Service Provider's failure to comply with this section in accordance with the "Limitation of Liability" provision set forth in the General Provisions - Information Technology.

E. The State at its option, may purchase additional transition services as agreed upon in the SOW and/or SLA.

F. During any period of suspension, the Service Provider shall not take any action to intentionally erase any State Data.

G. The Service Provider will impose no additional fees for access and retrieval of State Data by the State during the Transition Period.

H. After termination of the Contract and the prescribed retention period, the Service Provider shall securely dispose of all State Data in all forms. State Data shall be permanently deleted and shall not be recoverable, according to NIST-approved methods. Certificates of destruction shall be provided to the State.

9. BACKGROUND CHECKS:

As permitted or required by law, the Service Provider shall conduct criminal background checks and not utilize any staff, including subcontractors, to fulfill the obligations of the Contract who have been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or any misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Service Provider shall promote and maintain an awareness of the importance of securing the State's information among the Service Provider's employees and agents.

10. ACCESS TO SECURITY LOGS AND REPORTS:

A. **(For IaaS Only)** Upon request, the Service Provider shall provide reports to the State directly related to the infrastructure the Service Provider controls upon which the State account resides. Unless otherwise agreed to in the SLA, the Service Provider shall provide the State a history of all Application Program Interface (API) calls for the State account that includes the identity of the API caller, the time of the API call, the source IP address of the API caller, the request parameters and the response elements returned by the Service Provider. The report will be sufficient to enable the State to perform security analysis, resource change tracking and compliance auditing.

B. **(For PaaS Only)** Upon request, the Service Provider shall provide reports to the State in a format as specified in the SOW and/or SLA and agreed to by both the Service Provider and the State. Reports will include latency statistics, user access, user access IP address, user access history and security logs for all State files related to this Contract.

C. The Service Provider and the State recognize that security responsibilities are shared. The Service Provider is responsible for providing a secure infrastructure. The State is responsible for its secure guest operating system, firewalls and other logs captured within the guest operating system. Specific shared responsibilities are identified within the SOW and/or SLA.

11. CONTRACT AUDIT:

The Service Provider shall allow the State to audit conformance to the Contract terms. The State may perform this audit or Contract with a third party at its discretion and at the State's expense.

12. DATA CENTER AUDIT:

The Service Provider shall undergo an annual Statement on Standards for Attestation Engagements (SSAE) No. 16 Service Organization Control (SOC) 2 Type II audit of its data centers, or its successor at its own expense. The Service Provider shall provide a redacted version of the audit report and Contractor's plan to correct any negative findings upon request. The Service Provider may remove its proprietary information from the redacted version.

13. CHANGE CONTROL AND ADVANCE NOTICE:

The Service Provider shall give advance notice (as agreed to by the parties and included in the SOW and/or SLA) to the State of any upgrades (e.g., major upgrades, minor upgrades, system changes) that is expected to materially and negatively impact service availability and performance, as well as any planned downtime for such upgrades. A major upgrade is a replacement of hardware, software or firmware ware with a newer or better version in order to bring the system up to date or to improve its characteristics. It usually includes a new version number. Service Provider may change the features and functionality of the services, without degrading them, to make improvements, address security requirements and comply with changes in law.

14. SECURITY PROCESSES:

The Service Provider shall disclose its non-proprietary security processes and technical limitations to the State such that adequate protection and flexibility can be attained between the State and the Service Provider. The State and the Service Provider shall understand each other's roles and responsibilities, which shall be set forth in the SOW and/or SLA.

15. IMPORT AND EXPORT OF DATA:

The State shall have the ability to import or export data in whole or in part at its discretion without interference from the Service Provider. This includes the ability for the State to import or export data to or from other Service Providers.

16. RESPONSIBILITIES AND UPTIME GUARANTEE:

The Service Provider shall be responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. The technical and professional activities required for establishing, managing and maintaining the environment are the responsibility of the Service Provider. The system shall be available 24/7/365 (with agreed-upon maintenance downtime), and shall provide service to customers as defined in the SOW and/or SLA.

17. RIGHT TO REMOVE INDIVIDUALS:

The State shall have the right at any time to require the Service Provider remove from interaction with State any Service Provider representative who the State believes is detrimental to its working relationship with the Service Provider. The State shall provide the Service Provider with notice of its determination, and the reasons it requests the removal. The Service Provider shall not assign the person to any aspect of the Contract or future work orders without the State's consent.

18. BUSINESS CONTINUITY AND DISASTER RECOVERY:

The Service Provider shall provide a business continuity and disaster recovery plan and shall ensure that it achieves the State's Recovery Time Objective (RTO), as agreed to by the parties and set forth in the SOW and/or SLA.

19. WEB SERVICES:

(For PaaS Only) The Service Provider shall use Web services exclusively to interface with State Data in near real time when possible, or as mutually agreed in the SOW and/or SLA.