Cloud Service & Web Service Requirements and Data Use Agreement for the Division of Welfare and Supportive Services (DWSS)

THIS ATTACHMENT IS A SEPARATE AGREEMENT IN CONNECTION WITH THE MAIN CONTRACT BETWEEN: THE STATE of NEVADA, DIVISION OF WELARE AND SUPPORTIVE SERVICES (DWSS) AND CONTRACTOR.

This Cloud Service & Web Service AND Data Use Agreement ("CSWS-DUA") is effective as of the date of the Contract into which it is incorporated ("Effective Date"), by and between the DWSS and Contractor.

Purpose and Order of Precedence: The purpose of this CSWS-DUA is to facilitate access to, maintenance, storage, use, disclosure, or transmission of any Information/Data with Contractor, and describe Contractor's rights and obligations with respect to any Information/Data and the limited purposes for which the Contractor may receive, maintain, store, use, disclose or have access to this Information/Data. As of the Effective Date of this CSWS-DUA, if any provision of the Contract conflicts with this CSWS-DUA, this attachment holds authority.

1. With respect to ALL Information/Data, Contractor shall:

A. Exercise reasonable care and no less than the same degree of care the Contractor uses to protect its own confidential, proprietary and trade secret information to prevent Information/Data from being used in a manner not expressly authorized under this Contract or required by law. Contractor will access, create, maintain, receive, use, disclose, transmit or destroy ALL Information/Data in a secure fashion that protects against any reasonably anticipated threats or hazards to the security or integrity of such information or unauthorized uses. Contractor shall abide by the process and protocols described in this agreement for handling Information/Data is listed below, along with any updates.

B. Implement, update, and document privacy, security and breach notice policies and procedures and an incident response plan to address a breach, to comply with the privacy, security, and breach notice requirements of this DUA prior to conducting work under the Contract and upon request.

C. Certify persons with access to the Information/Data each have a demonstrated need to know and have access to Information/Data solely to the minimum extent necessary to accomplish the required tasks in this Contract and all the certified persons have agreed **in writing** to be bound by the disclosure and use limitations pertaining to the Information/Data contained in this CSWS-DUA. Contractor and its Subcontractors shall always maintain an updated, complete, accurate list of these persons, past and present, allowed access to the Information/Data and supply that list to DWSS at the start of and upon completion of the contract, as well as upon request.

D. Provide, and shall cause its Subcontractors and agents to provide, to DWSS written confirmation of compliance with controls and the terms and conditions of this CSWS-DUA with each submitted deliverable.

E. Provide a certificate of compliance with this CSWS-DUA to DWSS confirming Contractor's compliance with all provisions of this CSWS-DUA regarding the return and/or destruction of ALL Information/Data prior to this Contract's completion date.

F. Cooperate in any audit DWSS requests having provided advance written notice of the audit and potential for Contractor support, whether it is a state or federal audit, Contractor agrees/acknowledges that full participation and cooperation is critical in achieving a successful audit. Full participation and cooperation in an audit includes, but is not limited to, Contractor providing proof of system, media or device security and/or encryption to DWSS up to 14 days after DWSS' written request in response to a compliance investigation, audit, or the discovery of a breach. DWSS may also request production of proof of security at other times as necessary to satisfy state and federal monitoring requirements and audits.

G. Designate and identify a person or persons, as Privacy Official and Information Security Official, each of whom is authorized to act on behalf of Contractor and is responsible for the development and implementation of the privacy and security requirements in this CSWS-DUA. Contractor shall provide name and current address, phone number and e-mail address for such designated officials to DWSS upon execution of this CSWS-DUA and prior to any change. Upon written notice from DWSS, Contractor shall promptly remove and replace such official(s) if such official(s) is not performing the required functions.

2. Contractor shall comply with the following certifications, protocols, and processing:

A. Cloud Service Certification

1. Cloud Service providers utilized by DWSS must meet the Nevada State Standards for Cloud Computing (Document ID S.5.06.01 – Cloud Services) requirements based on the Service Type; Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), or Function as a Service (FaaS).

2. The State of Nevada provides documents to assist in assessing the service security requirements, based on the Service Type:
    a. Documents are located at Universal Resource Location (URL): https://it.nv.gov/Governance/Security/State_Security_Policies_Standards___Procedures
        i. S.5.06.01 Cloud Services
        ii. S.5.06.01.1F Cloud Services Assessment Worksheet

3. Service providers must be able to prove their security level by either:
    a. Completing the Cloud Services Assessment Worksheet for the provided Service Type; or
    b. Providing proof of certification by a third party, which proves the minimum requirement level has been implemented, as indicated by the Cloud Service Standard, based on Service Type, e.g. annual SOC 2 report.; or
    c. Proof of Security Level must be provided to the DWSS Information Security Officer (ISO) for evaluation and approval.

4. FEDRAMP Certification is Required, if:
    a. Transport, compute, or store Office of Child Support Enforcement (OSCE) information; or
    b. To connect with an Office of Child Support Enforcement (OCSE) information system (such as NVKIDS), that service provider must meet FEDRAMP certification.

c. Review the FEDRAMP website for more FEDRAMP program information: https://www.fedramp.gov.

B. TCP/IP Connection Protection (Cloud and Web Services)

1. Transmission of data between the Service Provider and DWSS must enforce TLS 1.2 (or greater) tunneling protocol using AES 256-bit (or stronger) encryption to protect data in transit.
    a. These standards are current as of 6/3/2021 and will be updated periodically, as State, Federal, and industry security standards improve.

2. Computers must use security certification to authenticate with other computers in the connection.
    a. Certificates can be signed by the respective company owning the Cloud system or provided by a third-party certification authority.
    b. Certificates must be created with 2048-bit keys (or greater).
        i. These standards are current as of 6/3/2021 and will be updated periodically, as State, Federal, and industry security standards improve.
    c. Certificates must expire every 12 months to prevent long-term connection authorizations without re-issuing of certificates.

3. Connection endpoints to DWSS networks must be limited in functionality to what is required, not desired:
    a. Normally, either endpoint can open a new connection or listen for connections, but not both.
        i. Typically, DWSS is set to listen, and the connecting party will initiate the connection as needed to transmit information.
    b. Both endpoints can be enabled to open new connections and listen for connections only if the systems involved are specifically required to utilizing both functions on the common connection.
        i. Example:
            1. System 1 connects to System 2 to exchange information after which the connection is terminated; and
            2. Sometime later System 1 calls back System 2 to respond.
            3. This would require both end points to open connections and listen for connections.
    c. Endpoints must NOT hold a consistent connection to the DWSS endpoint longer than is required to complete the transaction or transaction batch.
    d. The connecting system must be responsible to terminate its own connection when the service has completed the transaction(s) with DWSS and not be designed to rely upon the DWSS connection termination.
    e. Endpoints will forcibly be terminated from the DWSS side if a connection is idle for more than 30 minutes.

4. To allow connections to be initiated, DWSS will whitelist a primary IP address and a backup IP address.
    a. Production systems must be configured in a Server-to-Server configuration to allow only a single connection endpoint to be maintained into the DWSS system.

i. Multiple cloud service endpoints, such as a web server pool, should be configured to load-balance to a single IP address to connect to DWSS with. A backup IP address can also be configured if agreed upon between DWSS and the cloud service provider.

b. Other configurations must be presented, discussed, and approved by DWSS prior to attempting implementation or connection to DWSS systems.

C. Data Storage Protection

1. DWSS data stored within a non-DWSS owned system (Cloud Service) must:
    a. Be accessed only by Authorized Users as designated in writing by DWSS authorized personnel.
    b. Be protected by Least-Privileged User Rights concept utilizing Role-Based user permissions management for all users, that must access the DWSS data.
    c. Provide Multi-Factor Authentication (MFA) must be utilized by the Service Provider to allow further authentication of System Users who access DWSS data within the Service or Service Computing Environment.
        i. DWSS employees may access the Cloud Service from within the State network without MFA, if other authorization methods are in place between the State network and the Cloud Service.
        ii. A System User is defined as any person that is accessing DWSS data in a Cloud Service system.
    d. Provide Active Monitoring of the data storage for intrusion, modification, and/or destruction of the data storage system and data.
        i. Host intrusion systems and malware protection systems must be utilized, updated daily, and actively operated to protect the data.
        ii. Monitor for inbound and outbound communications traffic continuously for unusual or unauthorized activities and conditions.
    e. **Notification Requirement:** If federal agency's data (Data Owner) is being transmitted to a cloud system, the state and other federal agencies (Data Consumers), must be notified at least 45 days prior to transmitting federally owned data into a cloud environment.
    f. **Provide Data Isolation:** Software, data, and services that receive, process, store, or transmit data must be isolated within the cloud environment so that other cloud customers sharing physical or virtual space cannot access other customer data or applications.
    g. **Provide a Service Level Agreement (SLA)** to the agency to establish availability and reliability factors for the data.
    h. **Provide Data Encryption in Transit:** Data must be encrypted in transit within the cloud environment. All mechanisms used to encrypt data must be FIPS 140-2 compliant and operate using the FIPS 140-2 compliant module.
    i. P**rovide Data Encryption at Rest:** Data may need to be encrypted while at rest in the cloud, depending upon the security protocols inherent in the cloud. If the cloud environment cannot appropriately isolate data, encryption is a potential compensating control. All mechanisms used to encrypt data must be FIPS 140-2 compliant and operate using the FIPS 140-2 compliant module.

j. **Provide Persistence of Data in Relieved Assets:** Storage devices where data has resided must be securely sanitized or destroyed using methods acceptable by NSA and Central Security Service (CSS).

k. **Provide Risk Assessment:** The agency must conduct an annual assessment of the security risk on all information systems used for receiving, processing, storing, or transmitting data. For the annual assessment immediately prior to implementation of the cloud environment and at each annual risk assessment (or update to an existing risk assessment) thereafter, the agency must include the cloud environment.

l. **Provide Security Control Implementation:** Customer-defined security controls must be identified, documented, and implemented. The customer-defined security controls, as implemented, must comply with requirements of the data ownership.

D. Post Contract Data Removal

1. Data will not be allowed to remain in a vendor's system for more than 30 days past contract end date or previously agreed upon modified end date.

2. The vendor is responsible for proper handling of the data until the data has been moved and permanently deleted from the system and the system storage has been sanitized.

3. The system storage must be sanitized per requirement Persistence of Data in Relieved Assets above.

4. DWSS is responsible for instructing the vendor on how to, when, and where to move the data to an acceptable location and in an acceptable format to DWSS.
    a. This process must be resolved prior to the contract end date. Technology, data formats, and data storage systems will change over time, therefore this is best decided closer to the end of contract, rather than in the beginning.

E. Security Incident Reporting

1. Security Incident involving the DWSS system or the common interface between the Service Provider's Cloud System, or Web Service, and contractor must communicate with DWSS via email and audio or video call within one (1) hour of discovery with as much detail known at that time.

2. Security Incident in the system will constitute an Immediate Disconnection requirement from DWSS' network until the situation is contained and in control of the System Provider. This requirement is to minimize the potential of the incident agent being able to cross the network connection into DWSS's network systems.

3. A final incident report must be provided to and cooperatively discussed with DWSS within thirty (30) calendar days from the conclusion of the security incident.

4. Periodic incident discussions must be conducted between Contractor and DWSS, at least every five (5) calendar days, between the beginning of the security incident and the conclusion of the security incident. Daily communication is encouraged.

5. DWSS Office of Information Security, Contact Information:
    a. Attn: Office of Information Security, Division of Welfare and Supportive Services, State of Nevada
    b. Address: 1470 College Parkway, Carson City, NV 89706
    c. Email: welfsecurity@dwss.nv.gov
    d. Email/letter subject line: **Security Incident Notification involving DWSS Data or Interface at {Cloud Service Provider Name/Program Name}**

F. Re-Use of Data

1. Prohibit usage, transmission, or storage of data by vendor(s) for any reason other than what is explicitly set forth in the contract with the vendor. These prohibitions include, but are not limited to, any actions by vendor(s) that would result in profit creation from the data DWSS provides or is responsible for.

2. For data that DWSS does not own, DWSS must acquire written permission to share or alter the process outlined in an existing agreement for sharing their data with another vendor(s) for usage, transfer, and/or storage of that data. This usually requires new data sharing agreements or updating of existing data sharing agreements.

G. Failures to Comply and Repercussions (Cloud and Web Services)

1. Failure to maintain security to these standards will result in a review of the problem areas by the DWSS ISO and technical management and the Service Provider's technical management if the problems cannot be resolved and brought fully into specifications as soon as reasonably practicable but in any event within 30 calendar days.

2. DWSS is under strict Federal regulations for reporting data or system security breaches in a timely manner. Therefore, DWSS requires the same level of service from its vendors, in order to support DWSS' Federal requirements. Failure to report Data Breaches to the DWSS ISO and DWSS Privacy Officer within specified time frames will result in:
    a. Immediate Disconnection between DWSS networks and the Cloud/Web Service system; and
    b. Require of a review of reporting procedures with the Service Provider and DWSS ISO & Privacy Officer within three (3) working days.

3. Repeated occurrences of failures to maintain security standards or incident reporting can result in breach of contract.

4. DWSS' discretion controls in declaring a breach under 5 USC §552a (The Privacy Act), Nevada Revised Statute (NRS) 603A.020, 603A.210; and 603A220.

3. With respect to ALL Information/Data, Contractor shall NOT:

A. Attempt to re-identify or further identify Information/Data that has been deidentified or attempt to contact any persons whose records are contained in the Information/Data, except as expressly authorized under this Contract or required by law, without express written authorization from DWSS.

B. Engage in prohibited marketing or sale of this Information/Data. Contractor shall not share, publish, or otherwise release any findings or conclusions derived from any analysis of the Information/Data without **prior written approval** from DWSS.

C. Permit or enter into any agreement with a Subcontractor to create, receive, maintain, use, disclose, have access to or transmit Information/Data, on behalf of DWSS without **written permission** of DWSS, and requiring that Subcontractor execute either the CSWS-DUA Agreement or Contractor's own Subcontractor agreement that ensures the Subcontractor shall comply with the same safeguards and restrictions contained in this CSES-DUA for Information-Data. Contractor is directly responsible for its Subcontractors' compliance with, and enforcement of, this CSWS-DUA.

4. Data Breach Provisions:

A breach of PII, Federal Tax Information (FTI), or Social Security Administration data must be reported with the first consecutive hour of discovery to the DWSS Privacy Officer.

A. Initial Breach Notice: Contractor must provide details of the breach to the extent known to the Contractor, including, but not limited to:

1. The date the breach occurred;
2. The date of the Contractor and, if applicable, Subcontractor's discovery;
3. A brief description of the breach, including how it occurred and who is responsible (or hypothesis if not yet determined);
4. A brief description of the Contractor's investigations and the status of that investigation;
5. A description of the types and amount of Confidential Information involved;
6. Identification of and number of all individuals reasonably believed to be affected, including first and last name of the individual and if applicable, the legally authorized representative, last known address, age, telephone number, and email address if it is a preferred contact method;
7. Contractor's initial risk assessment of the Breach demonstrating whether individual or other notices are required by applicable law or this DUA for DWSS Privacy Officer approval, including an analysis of whether there is a low probability of compromise of the Confidential Information/PII or whether any legal exceptions to notification apply;
8. Contractor's recommendation as to the steps individuals and/or Contractor on behalf of individuals, should take to protect the individuals from potential harm, including Contractor's provision of notifications, credit protection, claims monitoring, and any specific protections for a Legally Authorized Representative to take on behalf of an individual with special capacity or circumstances;
9. The steps Contractor has taken to mitigate the harm or potential harm caused (including without limitation the provision of sufficient resources to mitigate);
10. The steps Contractor has taken, or will take, to prevent or reduce the likelihood of recurrence of a similar Breach;
11. Identify, describe or estimate of the persons, Workforce, Subcontractor, or individuals and any law enforcement that may be involved in the Breach;
12. A reasonable schedule for Contractor to provide regular updates regarding response to the Breach, but no less than every three (3) business days, or as otherwise directed by DWSS Privacy Officer in writing, including information about risk estimations, reporting, notification,

if any, mitigation, corrective action, root cause analysis and when such activities are expected to be completed; and

13. Any reasonably available, pertinent information, documents or reports related to a Breach that DWSS Privacy Officer requests following Discovery.

B. Breach Notification to Individuals and Reporting to the Authorities

1. DWSS Privacy Officer may direct the Contractor to provide Breach notification to individuals, regulators or third parties as specified by DWSS Privacy Officer following a Breach.

2. Contractor must comply with all applicable legal and regulatory requirements in time, manner, and content of any notification to individuals, regulators or third-parties, or any notice required by other state or federal authorities, including without limitation, notifications required by NRS 603A and The Privacy Act. Notice letters will be in the Contractor's name and on the Contractor's letterhead, unless otherwise directed by DWSS Privacy Officer and will contain information, including the name and title of the Contractor's representative, an e-mail address, and a toll-free telephone number for the individual to obtain additional information.

3. Contractor shall provide DWSS Privacy Officer with draft notifications for DWSS Privacy Officer approval prior to distribution and copies of distributed and approved communications.

4. Contractor shall have the burden of demonstrating to the DWSS Privacy Officer that any required notification was timely made by providing all information reasonably available to Contractor about the breach no later than 5 p.m. Pacific Time on the third business day after Discovery or a time within which the Discovery should have reasonably been made by the Contractor for a Breach of Confidential Information. To the extent possible, the information should include, but not be limited to:

    a. First name, Last Name, Mailing Address for each individual affected by the breach.

    b. Summary of the breach that Contractor would suggest to include with the notifications.

5. If DWSS Privacy Officer directs the Contractor to provide notifications, DWSS Privacy Officer shall, in the time and manner reasonably requested by the Contractor, cooperate, and assist with the Contractor's information requests in order to make such notifications.

C. Contractor shall, at the Contractor's expense, cooperate fully with DWSS Privacy Officer in investigating, mitigating to the extent practicable, and issuing notifications as directed by DWSS, for any Breach of Confidential Information.

D. Contractor shall make the confidential information in the Contractor's possession available pursuant to applicable law upon determination of a breach.

E. Contractor's obligation begins at the discovery of a breach and continues as long as related activity continues, until all effects of the breach are mitigated to DWSS Privacy Officer's satisfaction (the "incident response period").

5. General Provisions:

A. Ownership of Information/Data - Contractor acknowledges and agrees that the Information/Data is and shall remain the property of DWSS. Contractor agrees it acquires no title or rights to the Information/Data.

B. DWSS Commitment and Obligations - DWSS will not request Contractor to create, maintain, transmit, use, or disclose Personally Identifiable Information (PII) or other protected Information/Data in any manner that would not be permissible under applicable law if done by DWSS.

C. **DWSS Right to Inspection** - At any time, upon reasonable notice to the Contractor, DWSS, directly or through its agent, will have the right to inspect the facilities, systems, books and records of Contractor to monitor compliance with this CSWS-DUA. If DWSS determines that Contractor has violated this CSWS-DUA, DWSS shall have the right to immediately inspect the facilities, systems, books and records of Contractor for failure to properly secure the Information/Data in accordance with the CSWS-DUA. For purposes of this subsection, DWSS's agent(s) include, without limitation, any Executive agency in the State of Nevada, Legislative Auditors, the Office of the Attorney General of Nevada, the State Auditor's Office, outside consultants, any Federal oversight agency or its contractors, legal counsel or other designee.

D. Termination of CSWS-DUA; Survival - This CSWS-DUA will be effective on the date on which Contractor executes the Contract and will terminate upon termination of the Contract and as set forth herein, except for any provisions specifically mentioned herein that will survive termination. If the Contract is extended, this CSES-DUA is extended to run concurrent with the Contract.

(1) If DWSS determines that Contractor has violated a material term of this CSWS-DUA; DWSS may in its sole discretion:

(a) Exercise any of its rights including but not limited to reports, access and inspection under this CSWS-DUA and/or the Contract; or

(b) Require Contractor to submit to a corrective action plan, including a plan for monitoring and plan for reporting as DWSS may determine necessary to maintain compliance with this CSWS-DUA; or

(c) Provide Contractor with a reasonable period to cure the violation as determined by DWSS; or

(d) Terminate the CSWS-DUA and Contract immediately and seek relief in a court of competent jurisdiction in Carson City, Nevada.

Before exercising any of these options, DWSS will provide written notice to Contractor describing the violation and the action it intends to take.

(2) If neither termination nor cure is feasible, DWSS shall report the violation to the applicable regulatory authorities.

(3) The duties of Contractor or its Subcontractor under this CSWS-DUA survive the expiration or terminated by this CSWS-DUA.

E. Injunctive Relief:

(1) Contractor acknowledges and agrees that DWSS may suffer irreparable injury if Contractor or its Subcontractor fails to comply with any of the terms of this CSWS-DUA with respect to the Information/Data based on laws or regulations applicable to this Information/Data.

(2) Contractor further agrees that monetary damages may be inadequate to compensate DWSS for Contractor's or its Subcontractor's failure to comply. Accordingly, Contractor agrees that

DWSS will, in addition to any other remedies available to it at law or in equity, be entitled to seek injunctive relief without posting a bond and without the necessity of demonstrating actual damages, to enforce the terms of this CSWS-DUA.

F. Indemnification:

Contractor shall indemnify, defend and hold harmless DWSS and its respective elected officials, officers, employees, subcontractors, agents (including other state agencies acting on behalf of DWSS) or other persons employed/contracted by the State of Nevada (each of the foregoing hereinafter referred to as "Indemnified Party") against all actual and direct losses suffered by the Indemnified Party and all liability to third parties arising from or in connection with any breach of this CSWS-DUA or from any acts or omissions related to this CSWS-DUA by Contractor or its employees, directors, officers, Subcontractors, or agents or other persons employed/contracted by the Contractor. The duty to indemnify, defend and hold harmless is independent of the duty to insure. Upon demand, Contractor shall reimburse DWSS for any and all losses, liabilities, lost profits, fines, penalties, costs or expenses (including costs of required notices, investigation, and mitigation of a breach, fines or penalties imposed on an Indemnified Party by a regulatory authority, and reasonable attorneys' fees) which may be imposed upon any Indemnified Party to the extent caused by and which results from the Contractor's failure to meet any of its obligations under this CSWS-DUA. Contractor's obligation to defend, indemnify and hold harmless any Indemnified Party will survive the expiration or termination of this Contract and this CSWS-DUA.

G. Insurance:

(1) In addition to any insurance required in the Contract, at DWSS's option, DWSS may require Contractor to maintain, at its expense, the special and/or custom first- and third-party insurance coverages, including without limitation data breach, cyber liability, crime theft and notification expense coverages, with policy limits sufficient to cover any liability arising under this CSWS-DUA, naming the State of Nevada, acting through DWSS, as an additional named insured and loss payee, with primary and noncontributory status.

(2) Contractor shall provide DWSS with written proof that required insurance coverage is in effect, at the request of DWSS.

H. Governing Law: Jurisdiction: This Contract and the rights and obligations of the parties hereto shall be governed by, and construed according to, the laws of the State of Nevada, without giving effect to any principle of conflict-of-law that would require the application of the law of any other jurisdiction. The parties consent to the exclusive jurisdiction of and venue in the First Judicial District Court, Carson City, Nevada for enforcement of this Contract, and consent to personal jurisdiction in such court for any action or proceeding arising out of this Contract.

I. Entirety of the Contract:

This CSWS-DUA is incorporated by reference into the Contract and, together with the Contract, constitutes the entire agreement between the parties. No change, waiver, or discharge of obligations arising under those documents will be valid unless in writing and executed by the party against whom such change, waiver, or discharge is sought to be enforced.

I. Automatic Amendment and Interpretation:

Upon the effective date of any amendment or issuance of additional regulations to any law applicable to Information/Data, this CSWS-DUA will automatically be amended so that the obligations imposed on DWSS and/or Contractor remain in compliance with such requirements.

Any ambiguity in this CSWS-DUA will be resolved in favor of a meaning that permits DWSS and Contractor to comply with laws applicable to Information/Data.

J. Requests for Approval:
All notices and requests for approvals related to this CSWS-DUA must be directed to the DWSS Contracts Unit at dwsscontracts@dwss.nv.gov .

6. Response to 1.G – Contractor's Points of Contact

A. Contractors' Privacy Official

Name: _____
Current Street Address: _____
Phone Number: _____
Fax Number: _____
Email Address: _____

B. Contractors' Information Security Official

Name: _____
Current Street Address: _____
Phone Number: _____
Fax Number: _____
Email Address: _____

Independent Contractor	Date	Independent Contractor's Title
Robert Thompson	Date	Administrator, Division of Welfare and Supportive Services Title