Washington State **Department of Social & Health Services** *Transforming lives*	**CLIENT SERVICE CONTRACT** **DCS – Banking Services**	DSHS Contract Number: 2513-60204 Resulting From Solicitation Number: 2434-864
This Contract is between the State of Washington Department of Social and Health Services (DSHS) and the Contractor identified below.		Program Contract Number: Contractor Contract Number:

CONTRACTOR NAME	CONTRACTOR doing business as (DBA)	
CONTRACTOR ADDRESS	WASHINGTON UNIFORM BUSINESS IDENTIFIER (UBI)	DSHS INDEX NUMBER

CONTRACTOR CONTACT	CONTRACTOR TELEPHONE	CONTRACTOR FAX	CONTRACTOR E-MAIL ADDRESS

DSHS ADMINISTRATION	DSHS DIVISION	DSHS CONTRACT CODE
Economic Services Administration	Division of Child Support	3000XC-13

DSHS CONTACT NAME AND TITLE	DSHS CONTACT ADDRESS

DSHS CONTACT TELEPHONE	DSHS CONTACT FAX	DSHS CONTACT E-MAIL ADDRESS

IS THE CONTRACTOR A SUBRECIPIENT FOR PURPOSES OF THIS CONTRACT? No	ASSISTANCE LISTING NUMBER(S)

CONTRACT START DATE	CONTRACT END DATE	CONTRACT MAXIMUM AMOUNT
10/01/2025	09/30/2029	Fee For Service

EXHIBITS. The following Exhibits are attached and are incorporated into this Contract by reference:

☐ Exhibits (specify): Exhibit A - Data Security Requirements; Exhibit B - Confidentiality Statement - Non-DCS Employee; Exhibit C – Fee Schedule

☐ **No Exhibits.**

The terms and conditions of this Contract are an integration and representation of the final, entire and exclusive understanding between the parties superseding and merging all previous agreements, writings, and communications, oral or otherwise, regarding the subject matter of this Contract. The parties signing below represent that they have read and understand this Contract, and have the authority to execute this Contract. This Contract shall be binding on DSHS only upon signature by DSHS.

CONTRACTOR SIGNATURE	PRINTED NAME AND TITLE	DATE SIGNED
Draft - Please Do Not Sign		

DSHS SIGNATURE	PRINTED NAME AND TITLE	DATE SIGNED
Draft - Please Do Not Sign		

DSHS General Terms and Conditions

1. **Definitions**. The words and phrases listed below, as used in this Contract, shall each have the following definitions:

   a. "Central Contracts and Legal Services" means the DSHS central headquarters contracting office, or successor section or office.

   b. "Confidential Information" or "Data" means information that is exempt from disclosure to the public or other unauthorized persons under RCW 42.56 or other federal or state laws. Confidential Information includes, but is not limited to, Personal Information.

   c. "Contract" or "Agreement" means the entire written agreement between DSHS and the Contractor, including any Exhibits, documents, or materials incorporated by reference. The parties may execute this contract in multiple counterparts, each of which is deemed an original and all of which constitute only one agreement. E-mail or Facsimile transmission of a signed copy of this contract shall be the same as delivery of an original.

   d. "CCLS Chief" means the manager, or successor, of Central Contracts and Legal Services or successor section or office.

   e. "Contractor" means the individual or entity performing services pursuant to this Contract and includes the Contractor's owners, members, officers, directors, partners, employees, and/or agents, unless otherwise stated in this Contract. For purposes of any permitted Subcontract, "Contractor" includes any Subcontractor and its owners, members, officers, directors, partners, employees, and/or agents.

   f. "Debarment" means an action taken by a Federal agency or official to exclude a person or business entity from participating in transactions involving certain federal funds.

   g. "DSHS" or the "Department" means the state of Washington Department of Social and Health Services and its employees and authorized agents.

   h. "Encrypt" means to encode Confidential Information into a format that can only be read by those possessing a "key;" a password, digital certificate or other mechanism available only to authorized users. Encryption must use a key length of at least 256 bits for symmetric keys, or 2048 bits for asymmetric keys. When a symmetric key is used, the Advanced Encryption Standard (AES) must be used if available.

   i. "Personal Information" means information identifiable to any person, including, but not limited to, information that relates to a person's name, health, finances, education, business, use or receipt of governmental services or other activities, addresses, telephone numbers, Social Security Numbers, driver license numbers, other identifying numbers, and any financial identifiers.

   j. "Physically Secure" means that access is restricted through physical means to authorized individuals only.

   k. "Program Agreement" means an agreement between the Contractor and DSHS containing special terms and conditions, including a statement of work to be performed by the Contractor and payment to be made by DSHS.

   l. "RCW" means the Revised Code of Washington. All references in this Contract to RCW chapters or sections shall include any successor, amended, or replacement statute. Pertinent RCW chapters can be accessed at http://apps.leg.wa.gov/rcw/.

m. "Regulation" means any federal, state, or local regulation, rule, or ordinance.

n. "Secured Area" means an area to which only authorized representatives of the entity possessing the Confidential Information have access. Secured Areas may include buildings, rooms or locked storage containers (such as a filing cabinet) within a room, as long as access to the Confidential Information is not available to unauthorized personnel.

o. "Subcontract" means any separate agreement or contract between the Contractor and an individual or entity ("Subcontractor") to perform all or a portion of the duties and obligations that the Contractor is obligated to perform pursuant to this Contract.

p. "Tracking" means a record keeping system that identifies when the sender begins delivery of Confidential Information to the authorized and intended recipient, and when the sender receives confirmation of delivery from the authorized and intended recipient of Confidential Information.

q. "Trusted Systems" include only the following methods of physical delivery: (1) hand-delivery by a person authorized to have access to the Confidential Information with written acknowledgement of receipt; (2) United States Postal Service ("USPS") first class mail, or USPS delivery services that include Tracking, such as Certified Mail, Express Mail or Registered Mail; (3) commercial delivery services (e.g. FedEx, UPS, DHL) which offer tracking and receipt confirmation; and (4) the Washington State Campus mail system. For electronic transmission, the Washington State Governmental Network (SGN) is a Trusted System for communications within that Network.

r. "WAC" means the Washington Administrative Code. All references in this Contract to WAC chapters or sections shall include any successor, amended, or replacement regulation. Pertinent WAC chapters or sections can be accessed at http://apps.leg.wa.gov/wac/.

2. **Amendment.** This Contract may only be modified by a written amendment signed by both parties. Only personnel authorized to bind each of the parties may sign an amendment.

3. **Assignment.** The Contractor shall not assign this Contract or any Program Agreement to a third party without the prior written consent of DSHS.

4. **Billing Limitations.**

a. DSHS shall pay the Contractor only for authorized services provided in accordance with this Contract.

b. DSHS shall not pay any claims for payment for services submitted more than twelve (12) months after the calendar month in which the services were performed.

c. The Contractor shall not bill and DSHS shall not pay for services performed under this Contract, if the Contractor has charged or will charge another agency of the state of Washington or any other party for the same services.

5. **Compliance with Applicable Law and Washington State Requirements.**

a. **Applicable Law**. Throughout the performance of this Agreement, Contractor shall comply with all federal, state, and local laws, regulations, and executive orders to the extent they are applicable to this Agreement.

b. **Civil Rights and Nondiscrimination**. Contractor shall comply with all federal and state civil rights

and nondiscrimination laws, regulations, and executive orders to the extent they are applicable to this Agreement, including, but not limited to, and as amended, Titles VI and VII of the Civil Rights Act of 1964; Sections 503 and 504 of the Rehabilitation Act of 1973; the Americans with Disabilities Act (ADA); Executive Order 11246; the Health Insurance Portability and Accountability Act of 1996 (HIPAA); the Age Discrimination in Employment Act of 1967, the Age Discrimination Act of 1975, the Vietnam Era Veterans' Readjustment Assistance Act of 1974, and Chapter 49.60 of the Revised Code of Washington, Washington's Law Against Discrimination. These laws, regulations and executive orders are incorporated by reference herein to the extent that they are applicable to the Contract and required by law to be so incorporated.

In the event of the Contractor's noncompliance or refusal to comply with any applicable nondiscrimination laws, regulations, and executive orders, this Agreement may be rescinded, canceled, or terminated in whole or in part.

c. **Nondiscrimination.**

    (1) **Nondiscrimination Requirement**. During the term of this Contract, Contractor, including any subcontractor, shall not discriminate on the bases enumerated at RCW 49.60.530(3). In addition, Contractor, including any subcontractor, shall give written notice of this nondiscrimination requirement to any labor organizations with which Contractor, or subcontractor, has a collective bargaining or other agreement.

    (2) **Obligation to Cooperate**. Contractor, including any subcontractor, shall cooperate and comply with any Washington state agency investigation regarding any allegation that Contractor, including any subcontractor, has engaged in discrimination prohibited by this Contract pursuant to RCW 49.60.530(3).

d. **Certification Regarding Russian Government Contracts and/or Investments**. Contractor shall abide by the requirements of Governor Jay Inslee's Directive 22-03 and all subsequent amendments. The Contractor, by signature to this Contract, certifies that the Contractor is not presently an agency of the Russian government, an entity which is Russian-state owned to any extent, or an entity sanctioned by the United States government in response to Russia's invasion of Ukraine. The Contractor also agrees to include the above certification in any and all Subcontracts into which it enters. The Contractor shall immediately notify DSHS if, during the term of this Contract, Contractor does not comply with this certification. DSHS may immediately terminate this Contract by providing Contractor written notice if Contractor does not comply with this certification during the term hereof.

6. **Confidentiality.**

a. The Contractor shall not use, publish, transfer, sell or otherwise disclose any Confidential Information gained by reason of this Contract for any purpose that is not directly connected with Contractor's performance of the services contemplated hereunder, except:

    (1) as provided by law; or,

    (2) in the case of Personal Information, with the prior written consent of the person or personal representative of the person who is the subject of the Personal Information.

b. The Contractor shall protect and maintain all Confidential Information gained by reason of this Contract against unauthorized use, access, disclosure, modification or loss. This duty requires the Contractor to employ reasonable security measures, which include restricting access to the

Confidential Information by:

(1) Allowing access only to staff that have an authorized business requirement to view the Confidential Information.

(2) Physically Securing any computers, documents, or other media containing the Confidential Information.

(3) Ensure the security of Confidential Information transmitted via fax (facsimile) by:

    (a) Verifying the recipient phone number to prevent accidental transmittal of Confidential Information to unauthorized persons.

    (b) Communicating with the intended recipient before transmission to ensure that the fax will be received only by an authorized person.

    (c) Verifying after transmittal that the fax was received by the intended recipient.

(4) When transporting six (6) or more records containing Confidential Information, outside a Secured Area, do one or more of the following as appropriate:

    (a) Use a Trusted System.

    (b) Encrypt the Confidential Information, including:

        i. Encrypting email and/or email attachments which contain the Confidential Information.
        ii. Encrypting Confidential Information when it is stored on portable devices or media, including but not limited to laptop computers and flash memory devices.

Note: If the DSHS Data Security Requirements Exhibit is attached to this contract, this item, 6.b.(4), is superseded by the language contained in the Exhibit.

(5) Send paper documents containing Confidential Information via a Trusted System.

(6) Following the requirements of the DSHS Data Security Requirements Exhibit, if attached to this contract.

c. Upon request by DSHS, at the end of the Contract term, or when no longer needed, Confidential Information shall be returned to DSHS or Contractor shall certify in writing that they employed a DSHS approved method to destroy the information. Contractor may obtain information regarding approved destruction methods from the DSHS contact identified on the cover page of this Contract.

d. Paper documents with Confidential Information may be recycled through a contracted firm, provided the contract with the recycler specifies that the confidentiality of information will be protected, and the information destroyed through the recycling process. Paper documents containing Confidential Information requiring special handling (e.g. protected health information) must be destroyed on-site through shredding, pulping, or incineration.

e. Notification of Compromise or Potential Compromise. The compromise or potential compromise of Confidential Information must be reported to the DSHS Contact designated on the contract within one (1) business day of discovery. Contractor must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law or DSHS.

DSHS General Terms and Conditions

7. **Debarment Certification.** The Contractor, by signature to this Contract, certifies that the Contractor is not presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded by any Federal department or agency from participating in transactions (Debarred). The Contractor also agrees to include the above requirement in any and all Subcontracts into which it enters. The Contractor shall immediately notify DSHS if, during the term of this Contract, Contractor becomes Debarred. DSHS may immediately terminate this Contract by providing Contractor written notice if Contractor becomes Debarred during the term hereof.

8. **E-Signature and Records.** An electronic signature or electronic record of this Contract or any other ancillary agreement shall be deemed to have the same legal effect as delivery of an original executed copy of this Contract or such other ancillary agreement for all purposes.

9. **Governing Law and Venue.** This Contract shall be construed and interpreted in accordance with the laws of the state of Washington and the venue of any action brought hereunder shall be in Superior Court for Thurston County.

10. **Independent Contractor.** The parties intend that an independent contractor relationship will be created by this Contract. The Contractor and his or her employees or agents performing under this Contract are not employees or agents of the Department. The Contractor, his or her employees, or agents performing under this Contract will not hold himself/herself out as, nor claim to be, an officer or employee of the Department by reason hereof, nor will the Contractor, his or her employees, or agent make any claim of right, privilege or benefit that would accrue to such officer or employee.

11. **Inspection.** The Contractor shall, at no cost, provide DSHS and the Office of the State Auditor with reasonable access to Contractor's place of business, Contractor's records, and DSHS client records, wherever located. These inspection rights are intended to allow DSHS and the Office of the State Auditor to monitor, audit, and evaluate the Contractor's performance and compliance with applicable laws, regulations, and these Contract terms. These inspection rights shall survive for six (6) years following this Contract's termination or expiration.

12. **Maintenance of Records.** The Contractor shall maintain records relating to this Contract and the performance of the services described herein. The records include, but are not limited to, accounting procedures and practices, which sufficiently and properly reflect all direct and indirect costs of any nature expended in the performance of this Contract. All records and other material relevant to this Contract shall be retained for six (6) years after expiration or termination of this Contract.

    Without agreeing that litigation or claims are legally authorized, if any litigation, claim, or audit is started before the expiration of the six (6) year period, the records shall be retained until all litigation, claims, or audit findings involving the records have been resolved.

13. **Order of Precedence.** In the event of any inconsistency or conflict between the General Terms and Conditions and the Special Terms and Conditions of this Contract or any Program Agreement, the inconsistency or conflict shall be resolved by giving precedence to these General Terms and Conditions. Terms or conditions that are more restrictive, specific, or particular than those contained in the General Terms and Conditions shall not be construed as being inconsistent or in conflict.

14. **Severability.** If any term or condition of this Contract is held invalid by any court, the remainder of the Contract remains valid and in full force and effect.

15. **Survivability.** The terms and conditions contained in this Contract or any Program Agreement which, by their sense and context, are intended to survive the expiration or termination of the particular agreement shall survive. Surviving terms include, but are not limited to: Billing Limitations;

Confidentiality, Disputes; Indemnification and Hold Harmless, Inspection, Maintenance of Records, Notice of Overpayment, Ownership of Material, Termination for Default, Termination Procedure, and Treatment of Property.

16. **Contract Renegotiation, Suspension, or Termination Due to Change in Funding.**

    If the funds DSHS relied upon to establish this Contract or Program Agreement are withdrawn, reduced or limited, or if additional or modified conditions are placed on such funding, after the effective date of this contract but prior to the normal completion of this Contract or Program Agreement:

    a. At DSHS's discretion, the Contract or Program Agreement may be renegotiated under the revised funding conditions.

    b. At DSHS's discretion, DSHS may give notice to Contractor to suspend performance when DSHS determines that there is reasonable likelihood that the funding insufficiency may be resolved in a timeframe that would allow Contractor's performance to be resumed prior to the normal completion date of this contract.

       (1) During the period of suspension of performance, each party will inform the other of any conditions that may reasonably affect the potential for resumption of performance.

       (2) When DSHS determines that the funding insufficiency is resolved, it will give Contractor written notice to resume performance. Upon the receipt of this notice, Contractor will provide written notice to DSHS informing DSHS whether it can resume performance and, if so, the date of resumption. For purposes of this subsubsection, "written notice" may include email.

       (3) If the Contractor's proposed resumption date is not acceptable to DSHS and an acceptable date cannot be negotiated, DSHS may terminate the contract by giving written notice to Contractor. The parties agree that the Contract will be terminated retroactive to the date of the notice of suspension. DSHS shall be liable only for payment in accordance with the terms of this Contract for services rendered prior to the retroactive date of termination.

    c. DSHS may immediately terminate this Contract by providing written notice to the Contractor. The termination shall be effective on the date specified in the termination notice. DSHS shall be liable only for payment in accordance with the terms of this Contract for services rendered prior to the effective date of termination. No penalty shall accrue to DSHS in the event the termination option in this section is exercised.

17. **Waiver.** Waiver of any breach or default on any occasion shall not be deemed to be a waiver of any subsequent breach or default. Any waiver shall not be construed to be a modification of the terms and conditions of this Contract. Only the CCLS Chief or designee has the authority to waive any term or condition of this Contract on behalf of DSHS.

Additional General Terms and Conditions – Client Service Contracts:

18. **Advance Payment**. DSHS shall not make any payments in advance or anticipation of the delivery of services to be provided pursuant to this Contract.

19. **Construction**. The language in this Contract shall be interpreted as to its fair meaning and not strictly for or against any party. Any rule of construction to the effect that ambiguities are to be resolved against the drafting party shall not apply in interpreting this Contract.

20.   **Contractor Certification Regarding Ethics**. The Contractor certifies that the Contractor is now, and shall remain, in compliance with Chapter 42.52 RCW, Ethics in Public Service, throughout the term of this Contract.

21.   **Health and Safety**. Contractor shall perform any and all of its obligations under this Contract in a manner that does not compromise the health and safety of any DSHS client with whom the Contractor has contact.

22.   **Indemnification and Hold Harmless**

   a.   The Contractor shall be responsible for and shall indemnify, defend, and hold DSHS harmless from any and all claims, costs, charges, penalties, demands, losses, liabilities, damages, judgments, or fines, of whatsoever kind of nature, arising out of or relating to a) the Contractor's or any Subcontractor's performance or failure to perform this Contract, or b) the acts or omissions of the Contractor or any Subcontractor.

   b.   The Contractor's duty to indemnify, defend, and hold DSHS harmless from any and all claims, costs, charges, penalties, demands, losses, liabilities, damages, judgments, or fines shall include DSHS' personnel-related costs, reasonable attorney's fees, court costs, and all related expenses.

   c.   The Contractor waives its immunity under Title 51 RCW to the extent it is required to indemnify, defend, and hold harmless the State and its agencies, officials, agents, or employees.

   d.   Nothing in this term shall be construed as a modification or limitation on the Contractor's obligation to procure insurance in accordance with this Contract or the scope of said insurance.

23.   **Industrial Insurance Coverage**. The Contractor shall comply with the provisions of Title 51 RCW, Industrial Insurance. If the Contractor fails to provide industrial insurance coverage or fails to pay premiums or penalties on behalf of its employees, as may be required by law, DSHS may collect from the Contractor the full amount payable to the Industrial Insurance accident fund. DSHS may deduct the amount owed by the Contractor to the accident fund from the amount payable to the Contractor by DSHS under this contract, and transmit the deducted amount to the Department of Labor and Industries, (L&I) Division of Insurance Services. This provision does not waive any of L&I's rights to collect from the Contractor

24.   **Notice of Overpayment**. If the Contractor receives a vendor overpayment notice or a letter communicating the existence of an overpayment from DSHS, the Contractor may protest the overpayment determination by requesting an adjudicative proceeding. The Contractor's request for an adjudicative proceeding must:

   a.   Be received by the Office of Financial Recovery (OFR) at Post Office Box 9501, Olympia, Washington 98507-9501, within twenty-eight (28) calendar days of service of the notice;

   b.   Be sent by certified mail (return receipt) or other manner that proves OFR received the request;

   c.   Include a statement as to why the Contractor thinks the notice is incorrect; and

   d.   Include a copy of the overpayment notice.

   e.   Timely and complete requests will be scheduled for a formal hearing by the Office of Administrative Hearings. The Contractor may be offered a pre-hearing or alternative dispute resolution conference in an attempt to resolve the overpayment dispute prior to the hearing.

Failure to provide OFR with a written request for a hearing within twenty-eight (28) days of service of a vendor overpayment notice or other overpayment letter will result in an overpayment debt against the Contractor. DSHS may charge the Contractor interest and any costs associated with the collection of this overpayment. DSHS may collect an overpayment debt through lien, foreclosure, seizure and sale of the Contractor's real or personal property; order to withhold and deliver; or any other collection action available to DSHS to satisfy the overpayment debt.

25. **Subcontracting**. Except as otherwise provided in this Contract, the Contractor shall not subcontract any of the contracted services without the prior approval of DSHS. Contractor is responsible to ensure that all terms, conditions, assurances and certifications set forth in this Contract are included in any and all Subcontracts, unless an exception to including a particular term or terms has been approved in advance by the CCLS Chief. Any failure of Contractor or its subcontractors to perform the obligations of this Contract shall not discharge the Contractor from its obligations hereunder or diminish DSHS' rights or remedies available under this Contract.

26. **Subrecipients**.

a. General. If the Contractor is a subrecipient of federal awards as defined by 2 CFR Part 200 and this Agreement, the Contractor shall:

(1) Maintain records that identify, in its accounts, all federal awards received and expended and the federal programs under which they were received, by Assistance Listing Numbers (ALN) title and number, award number and year, name of the federal agency, and name of the pass-through entity;

(2) Maintain internal controls that provide reasonable assurance that the Contractor is managing federal awards in compliance with laws, regulations, and provisions of contracts or grant agreements that could have a material effect on each of its federal programs;

(3) Prepare appropriate financial statements, including a schedule of expenditures of federal awards;

(4) Incorporate 2 CFR Part 200, Subpart F audit requirements into all agreements between the Contractor and its Subcontractors who are subrecipients;

(5) Comply with the applicable requirements of 2 CFR Part 200, including any future amendments to 2 CFR Part 200, and any successor or replacement Office of Management and Budget (OMB) Circular or regulation; and

(6) Comply with the Omnibus Crime Control and Safe streets Act of 1968, Title VI of the Civil Rights Act of 1964, Section 504 of the Rehabilitation Act of 1973, Title II of the Americans with Disabilities Act of 1990, Title IX of the Education Amendments of 1972, The Age Discrimination Act of 1975, and The Department of Justice Non-Discrimination Regulations, 28 C.F.R. Part 42, Subparts C.D.E. and G, and 28 C.F.R. Part 35 and 39. (Go to https://ojp.gov/about/offices/ocr.htm for additional information and access to the aforementioned Federal laws and regulations.)

b. Single Audit Act Compliance. If the Contractor is a subrecipient and expends $750,000 or more in federal awards from any and/or all sources in any fiscal year, the Contractor shall procure and pay for a single audit or a program-specific audit for that fiscal year. Upon completion of each audit, the Contractor shall:

      (1) Submit to the DSHS contact person the data collection form and reporting package specified in 2 CFR Part 200, Subpart F, reports required by the program-specific audit guide (if applicable), and a copy of any management letters issued by the auditor;

      (2) Follow-up and develop corrective action for all audit findings; in accordance with 2 CFR Part 200, Subpart F; prepare a "Summary Schedule of Prior Audit Findings" reporting the status of all audit findings included in the prior audit's schedule of findings and questioned costs.

   c. Overpayments. If it is determined by DSHS, or during the course of a required audit, that the Contractor has been paid unallowable costs under this or any Program Agreement, DSHS may require the Contractor to reimburse DSHS in accordance with 2 CFR Part 200.

27.   **Termination for Convenience.** DSHS may terminate this Contract in whole or in part when it is in the best interest of DSHS by giving the Contractor at least thirty (30) calendar days' written notice. The Contractor may terminate this Contract for convenience by giving DSHS at least thirty (30) calendar days' written notice addressed to DSHS at the address listed on page 1 of this Contract.

28.   **Termination for Default**. The CCLS Chief may immediately terminate this Contract for default, in whole or in part, by written notice to the Contractor if DSHS has a reasonable basis to believe that the Contractor has:

   a. Failed to meet or maintain any requirement for contracting with DSHS;

   b. Failed to protect the health or safety of any DSHS client pursuant to the section entitled Health and Safety of this Contract;

   c. Failed to perform under, or otherwise breached, any term or condition of this Contract; and/or

   d. Violated any applicable law or regulation.

If it is later determined that the Contractor was not in default, the termination shall be considered a termination for convenience.

29.   **Termination or Expiration Procedure**. The following terms and conditions apply upon Contract termination or expiration:

   a. The Contractor shall cease to perform any services required by this Contract as of the effective date of termination or expiration.

   b. If the Contract is terminated, the Contractor shall comply with all instructions contained in the termination notice.

   c. The Contractor shall immediately deliver to the DSHS contact named on page one of this Contract, or to his or her successor, all DSHS property in the Contractor's possession. The Contractor grants DSHS the right to enter upon the Contractor's premises for the sole purpose of recovering any DSHS property that the Contractor fails to return within ten (10) calendar days of the effective date of termination or expiration of this Contract. Upon failure to return DSHS property within ten (10) calendar days, the Contractor shall be charged with all reasonable costs of recovery, including transportation.

   d. DSHS shall be liable only for payment required under the terms of this Contract for service rendered up to the effective date of termination or expiration.

e.   DSHS may withhold a sum from the final payment to the Contractor that DSHS determines necessary to protect DSHS against loss or additional liability.

f.   The rights and remedies provided to DSHS in this Section are in addition to any other rights and remedies provided at law, in equity, and/or under this Contract, including consequential and incidental damages.

30.   **Treatment of Client Property**. Unless otherwise provided, the Contractor shall ensure that any adult client receiving services from the Contractor has unrestricted access to the client's personal property. The Contractor shall not interfere with any adult client's ownership, possession, or use of the client's property. The Contractor shall provide clients under age eighteen (18) with reasonable access to their personal property that is appropriate to the client's age, development, and needs. Upon termination of services to a client, the Contractor shall immediately release to the client and/or the client's guardian or custodian all of the client's personal property.

31.   **Treatment of Property**. All property purchased or furnished by DSHS for use by the Contractor during this Contract term shall remain with DSHS. Title to all property purchased or furnished by the Contractor for which the Contractor is entitled to reimbursement by DSHS under this Contract shall pass to and vest in DSHS. The Contractor shall protect, maintain, and insure all DSHS property in its possession against loss or damage and shall return DSHS property to DSHS upon Contract termination or expiration.

32.   **Taxes**.

a.   Where required by statute or regulation, Contractor shall pay for and maintain in current status all taxes that are necessary for Contract performance. DSHS will pay sales or use taxes, if any, imposed on the services and materials acquired hereunder. Contractor must pay all other taxes including without limitation Washington Business and Occupation Tax, other taxes based on Contractor's income or gross receipts, or personal property taxes levied or assessed on Contractor's personal property. DSHS, as an agency of Washington State government, is exempt from property tax.

b.   Contractor shall complete registration with the Washington State Department of Revenue and be responsible for payment of all taxes due on payments made under this Contract in accordance with the requirements of Title 82 RCW and Title 458 WAC. Out-of-state Contractors must contact the Department of Revenue to determine whether they meet criteria to register and establish an account with the Department of Revenue. Refer to WAC 458-20-101 (Tax registration and tax reporting) and call the Department of Revenue at 800-647-7706 for additional information. When out-of-state Contractors are not required to collect and remit sales tax, DSHS shall be responsible for paying use tax, if applicable, directly to the Department of Revenue.

c.   All payments accrued on account of payroll taxes, unemployment contributions, any other taxes, insurance, or other expenses for Contractor or Contractor's staff shall be Contractor's sole responsibility.

33.   **Preventing Disruption of Adult Care, Mental Health, Addiction, Disability Support, or Youth Services Due to Labor Management Disputes and Employee Unrest.**

Washington law requires that all services, direct or ancillary, for adult care, mental health, addiction, disability support, and youth services, be warranted by the Contractor providing those services against disruption. Contractor and DSHS agree that disruptions to these services such as strikes, walk-offs, sick-ins, slowdowns, or any other such action designed to pressure Contractor's management to meet

labor, workforce, or subcontractor demands ("Economic or Industrial Action") are covered under this warranty.

If this Contract includes adult care, mental health, addiction, disability support, or youth services, Contractor agrees to execute and maintain one or more of the following mandatory contractual commitments through the life of the Contract:

a. An agreement between the Contractor and any exclusive representative labor organization representing the employees performing the contracted services. This agreement must contain a provision prohibiting Economic or Industrial Action on the part of all parties. This agreement must also include a process for the resolution of disputes between them; or

b. An agreement between the Contractor and any labor organization seeking to represent the employees performing the contracted services. This agreement must contain a provision prohibiting the parties from causing, promoting, or encouraging Economic or Industrial Action, or other disruptive activity. This agreement must also include a process for resolution of disputes between parties.

Contractor must notify DSHS if it is unable to form a compliant agreement with a labor organization within 30 days of executing this Contract.

If services under this Contract are interrupted due to Contractor's failure to maintain one or more of the required contractual commitments listed above, DSHS may immediately terminate, suspend, or revoke this Contract for default, and arrange for the provision of services by other means. Contractor shall provide reimbursement of the actual costs to DSHS arising out of the inadequacy of the warranty provided by the Contractor.

34. **Mandatory Individual Arbitration and Class or Collective Action Waiver as a Condition of Employment.**

   a. "Mandatory Individual Arbitration Clause" or "Class or Collective Action Waiver" means an arbitration clause or waiver in an employment contract which precludes Contractor's employees from resolving employment disputes with their employer through class or collective proceedings in federal court. Instead, employees must bring individualized arbitration proceedings against their employer to resolve any employment disputes.

   b. The Contractor, by signature to this Contract, certifies that the Contractor does not require Contractor's employees to agree to, as a condition of employment, a Mandatory Individual Arbitration Clause or Class or Collective Action Waiver.

   c. Contractor must notify DSHS within ten (10) business days if, during the term of this Contract, Contractor requires Contractor's employees to agree to, as a condition of employment, a Mandatory Individual Arbitration Clause or Class or Collective Action Waiver.

   d. If Contractor, during the term of this contract, requires Contractor's employees to agree to, as a condition of employment, a Mandatory Individual Arbitration Clause or Class or Collective Action Waiver, DSHS reserves the right to terminate this contract, per the General Terms and Conditions Section regarding Termination for Convenience.

Special Terms and Conditions

1. **Definitions Specific to Special Terms**. The words and phrases listed below, as used in this Contract, shall each have the following definitions:

   a. "ACH Rules or Nacha Rules" means the operating rules of the National Automated Clearing House Association, including all appendices and formal rules interpretations. Terms uses in reference to ACH processing in this Contract will have the same definition as they do in the Nacha Rules.

   b. "Cardholder" means a person who receives disbursements from a client and who is enrolled by the client in the debit card program and receives a card.

   c. "Division of Child Support (DCS)" means the Division within DSHS responsible for administering the state and federal child support program for the state of Washington.

   d. "Financial Institution" means a state or federally chartered depository institution, such as a bank, savings and loan, or credit union.

   e. "Flat File" means a file that consists of fixed length records, each of which is comprised of one or more fields of fixed length and position.

   f. "Image Cash Letter (ICL) means a check processing system that enables financial institutions and corporations to image paper items and transmit them electronically to the bank for deposit and clearing.

   g. "Interactive Voice Response" means a system for accessing account information.

   h. "International ACH Transaction (IAT)" means the Standard Entry Class code used for International corporate or consumer ACH credit or debit transactions.

   i. "International Wire Transfer" means the transfer of money to a financial institution in another country.

   j. "Non-Sufficient Funds (NSF)" means inadequate funds available to pay a check or ACH debit item.

   k. "Offshore" means outside of the United States territories, embassies, or military installations.

   l. "Positive Pay" means a fraud protection service that financial institutions offer businesses to help prevent check fraud.

   m. "Preauthorized Bill Payment" means an ACH debit application that deducts funds from a consumer's account for payment of an obligation.

   n. "Pre-Notification" means a zero dollar entry sent prior to the first live ACH transaction to notify the receiving depository financial institution of future payments and verify account information.

   o. "Prepaid Debit Card means a re-loadable payment mechanism used to deliver payments to individuals. The value of the payments is stored on the card.

   p. "Settlement Date" means the date an exchange of funds with respect to an entry is reflected on the books of the Federal Reserve Bank(s).

   q. "Standard Entry Class Codes" means three (3) character codes assigned to transactions to identify the type of transaction submitted to the ACH.

r. "Universal Payment Identification Code (UPIC)" means an identifier (or banking address) for a bank account in the United States used to receive electronic payments. It protects sensitive bank account information.

2. **Purpose**. The purpose of this Contract is for the Contractor to provide the Division of Child Support (DCS) with banking services for the collection and distribution of child support as provided in DSHS Request for Proposal (RFP) # 2434-864.

   a. DSHS enters into this Contract as the result of DSHS RFP 2434-864.

      (1) DSHS incorporates by reference DSHS RFP # 2434-864, including all Amendments and Exhibits.

      (2) DSHS incorporates by reference, the Contractor's written response to DSHS RFP # 2434-864.

3. **Period of Performance**.

   a. The Initial Term of this Contract shall be for four (4) years, as outlined on page one (1) of this Contract.

   b. This Contract may be extended upon mutual assent of both parties for three (3) two year terms.

   c. The total Period of Performance for this Contract shall not exceed ten (10) years.

4. **Statement of Work**. The Contractor shall provide the services and staff, and otherwise do all things necessary for or incidental to the performance of work, as set forth below:

   a. Account, ACH, and Reconciliation:

      DSHS is seeking the following banking services. Project work for all account services required in Section 3.a. Project Scope should begin on the first day of the contract between the financial institution and DCS. All bank account treasury services required must be installed and fully operational on or before October 1, 2025.

      The financial institution must cooperate in the transition of all bank services to another financial institution if they are not awarded subsequent contract at the end of this agreement. If the financial institution chooses not to pursue a subsequent contract at the end of this agreement, they must notify DCS at least twelve (12) months prior and must cooperate with the transition of all bank services to another financial institution.

      (1) This solicitation document requires that the successful bidder establish a minimum of four (4) zero-balance accounts and one (1) concentration account. The accounts will be in the name and Tax ID of Washington State Department of Social and Health Services, Division of Child Support (DSHS/DCS). At the end of each banking day the financial institution shall transfer account balances, whether deposit or disbursement, to the concentration account.

      New DCS accounts may be opened or accounts may be closed during the contract period by authorization of DCS. All new accounts will be subject to the terms and conditions of the contract.

      (2) The financial institution shall provide normal banking services associated with a public funds demand deposit account and analysis services.

Special Terms and Conditions

(3) The financial institution shall provide DCS with a toll-free number for access to bank staff that are dedicated, in whole or in part, to business conducted by DCS. Bank staff must be available between the hours of 6:30 AM and 5:30 PM Pacific Standard Time. In addition, the financial institution shall provide a problem resolution process and escalation protocol.

(4) The financial institution shall assign a single primary account representative for banking issues.

(5) The financial institution must be able to accept same day deposits delivered to branches or cash vaults in the following areas in Washington State:

(a) Olympia;

(b) Everett;

(c) Kennewick;

(d) Seattle;

(e) Spokane;

(f) Tacoma'

(g) Vancouver;

(h) Wenatchee; and

(i) Yakima.

(6) DCS may use 3 digit codes in the Auxiliary On-Us field of the deposit slips to identify the DCS location making the deposit. The financial institution warrants that deposits made at authorized branches of the financial institution shall be identified through the financial institution's deposit reporting system by DCS location code.

(7) The financial institution must be able to accept deposits through Image Cash Letter depository services via SFTP or Internet. If the financial institution has image quality requirements beyond the industry standard, they need to clarify what is different.

(8) The financial institution shall provide DCS with the foreign exchange rate for agreed upon foreign currencies to include at a minimum Canadian, British Pounds, and Euro, each business day morning, no later than 7:00 AM PST by email. This rate will be honored for all checks deposited that day which have the rate written upon them or the deposit slip(s).

(9) The financial institution shall credit all deposits, U. S. and Foreign, to the DCS account on the same day of receipt at the financial institution.

(10) The financial institution shall provide DCS with copies/images of deposited checks upon request, at no charge.

(11) The financial institution shall provide DCS with deposit slips, electronic and hand endorsement stamps printed to DCS specifications at cost.

(12) The financial institution shall allow deposit and disbursement corrections and transfers

initiated by DCS to be communicated by fax, e-mail, letter, telephone, and/or online banking services.

(13)   The financial institution shall include a DCS reference number on all deposit and disbursement adjustments upon request by DCS.

(14)   The financial institution must provide services to process incoming and outgoing domestic and international wire transfers.

(15)   The financial institution must have incoming and outgoing ACH processing capabilities for all National Automated Clearinghouse Association (NACHA) Standard Entry Class Codes (SEC), including International ACH Transactions (IAT).

(16)   The financial institution must be capable of processing ACH origination files containing multiple batches with unique company batch header identification codes and multiple ACH SEC codes for both consumer and corporate credit and debit transactions.

(17)   The financial institution must be able to settle ACH credit or debit origination files at the file level as opposed to the batch level for the origination company code associated with the transactions.

(18)   The financial institution shall inform DSHS of updates and changes to the ACH Rules.

(19)   The financial institution must support use of a UPIC for processing all incoming ACH transactions.

(20)   The financial institution shall provide custom translation of EDI/ACH files sent by DCS customers and other states. This service will require the financial institution to receive and interpret EDI/ACH files received through the ACH system and build an agreed upon DCS proprietary flat file that includes all pertinent payment detail and addenda information. The translated file will be retrieved the financial institution by DCS using a SFTP Client.

(21)   The financial institution shall provide Business eCheck blocks, ACH and check filters, and/or ACH and check blocks on accounts.

(22)   The financial institution shall ensure deposited checks and ACH debit items returned for non-sufficient Funds (NSF) and Funds Not Collected will be automatically presented for collection a second time. NSF checks and ACH items returned a second time will be debited against the demand deposit account of original deposit. All items returned as dishonored will be provided to DCS within three (3) working days, at no charge.

(23)   The financial institution shall provide DCS via SFTP or Internet, ACH Return Reports for all ACH Notice of Corrections and Returned ACH debits, disbursements and pre-notes the day following the day of the return or correction at no charge to DCS. The financial institution must provide the following information in the notice:

(a) DCS Company ID;

(b) Customer Name;

(c) Bank Account number;

(d) Return reason; and

(e) Amount returned.

(24)   Requests for ACH adjustments (for example, transaction or file reversals, deletes, etc.) shall be available through Internet ACH services, email, or fax.

(25)   The financial institution must be able to receive a Check Issuance File from DCS (or contracted check printing vendor) via SFTP or Internet.

(26)   Financial Institution shall provide Positive Pay, Payee Positive Pay, and Stale Dated maintenance services to prevent fraud.

(27)   DCS shall not be liable for checks that have been fraudulently altered or have forged endorsements while utilizing fraud protection services.

(28)   Financial Institution will provide a file of the weekly summary of checks paid via SFTP or Internet at no charge to DCS. The data must be received by DCS by the second business day of the week following the reporting date.

(29)   The financial institution shall make available copies of redeemed checks, front and back, via SFTP or Internet, upon request.

(30)   The financial institution shall provide DCS with software that will enable DCS to view and export in PDF or Group 4 Tiff file format the images of redeemed checks at no charge to DCS.

(31)   The financial institution shall provide Secure Internet stop payment processing with a maximum two (2) hour response time.

(32)   The financial institution shall provide an electronic summary of checks stopped through SFTP or Internet. This report, at minimum, shall include:

(a) Check number;

(b) Check amount; and

(c) Date check was stopped.

(33)   The financial institution must be able to issue a cashier's check drawn on the DCS account upon request for immediate pickup by designated payee at branch locations.

(34)   The financial institution shall ensure the existing DCS ACH credit and debit batch templates will transfer in their entirety (be importable) into the contractor's bank system.

(35)   The financial institution shall provide services to consolidate payments made to DCS through consumer bill-payment service providers for payments initiated by consumers using various banks, financial institutions, collection agencies, credit counseling agencies, or walk-in payment centers. Funds are to be converted to a single ACH settlement to the DSHS/DCS bank account and an agreed upon DCS proprietary flat file built that includes all pertinent payment details. The translated file will be retrieved from the financial institution by DCS using a SFTP Client.

Special Terms and Conditions

(36)   The financial institution must provide Single Location Secure Online Banking Services. The online banking must provide the minimum services:

   (a) Ability to create multiple levels of security, allowing a minimum of twenty (20) higher level security access devices, if required, at no charge to DCS;

   (b) Allow access by multiple users in various locations at the same time;

   (c) Ability to control user access to accounts and services;

   (d) Ensure DCS accounts are secure and protected;

   (e) Maintain Positive Pay systems to prevent fraud;

   (f) Provide Account and General ledger reconciliation;

   (g) System Created remittance file for incoming payments resulting from DCS-initiated ACH debit transactions;

   (h) Ability to create, manage, save, and reuse ACH Database templates;

   (i) Ability to view and manage DCS account activity

   (j) Ability to transfer money between accounts;

   (k) Allow Authorized Users to initiate both domestic and international ACH and wire transfer;

   (l) Provide NACHA formatting, supporting pre-notifications for all NACHA Standard Entry Class Codes, including IAT;

   (m) Allow Users to access, review and print check images, reports and statements;

   (n) Guarantee data recovery from damaged, failed, corrupted, or inaccessible online database;

   (o) Capability to create custom reports;

   (p) Provide access to online help and/or printed manuals; and

   (q) Provide customer support, with a toll free support line, and available email and remote diagnostics between the hours of 6:30 a.m. and 5:30 p.m. PST.

   The on-line system must adhere to widely accepted industry standards, passed independent audit testing, and the requirements of Sect. 3.a.34. above.

(37)   The financial institution shall provide SFTP process or Internet for account data on a daily basis for current and prior day information. This information shall include account numbers and account activity in detail and summary format and shall be available no later than 6:30 AM PST each business day.

(38)   The financial institution shall provide weekly check disbursement account statements. The weekly statements shall include:

(a) The date checks are redeemed;

(b) Check number;

(c) Amount of the check;

(d) Reconciliation of check register to weekly disbursement statement with errors identified and corrected; and

(e) Details regarding ZBA miscellaneous debits and credits.

(39)   The financial institution shall provide a monthly statement of the previous month's account(s) activity by the 8th Business Day of the following month. The monthly deposit account statements shall include daily summaries of deposits, adjustments and transfers for the reporting month. Deposit account statements shall also include an account summary that summarizes deposit activity by location code. The monthly EFT disbursement account statements shall include daily summaries of all disbursements, adjustments and transfers for the reporting month. Monthly statements shall be available through SFTP or Internet at no charge to DCS.

(40)   The financial institution shall provide cash management services including, but not limited to investment of balances allowed by state law, cash flow analysis, float information and a detailed audit trail of all transactions.

(41)   The financial institution will allow DCS to submit billings through the financial institution with payments made by the financial institution from excess earnings credit on DCS account(s). Billings may include, but are not limited to, deposit slips and or bags, endorsement plate costs, and ACH/financial institution publications. The financial institution shall provide a Financial Institution Routing Directory download code and other items as deemed appropriate.

(42)   All banking fees shall be included on the monthly account analysis. The analysis shall be available through SFTP or Internet at no charge to DCS and shall include a summary of all accounts and detail by account. Each section shall include:

(a) Service Code;

(b) Service definition;

(c) Volume for the month;

(d) Price per item;

(e) Total cost for the month; and

(f) A section that includes current month and year to date information on:

   i.   Average ledger balance;

   ii. Float;

   iii. Average collected balance;

iv. Net collected balance;

v. Balance available for earnings;

vi. Service charge detail;

vii. Earnings credit;

viii. Earnings rate; and

ix. Total Fees.

(43)   The financial institution shall provide competitive earnings credit to partially offset fees. Earnings credits are to be carried from period-to-period and year-to-year. Accumulated fees will be payable after the end of the fiscal year closing June 30, within 30 days of receipt of the bill.

(44)   Bidder shall provide a plan describing approach and methodology regarding conversion and transition phases.

(45)   Financial institutions may provide alternative solutions that are more efficient, cost-effective, and/or a more secure approach to the request services.

(46)   Financial institution is expected to provide leadership in the development and implementation of new technologies related to banking services throughout the term of the Agreement.

(47)   The financial institution shall not phase out technology during the contract period without allowing DCS acceptable replacement options.

b. DCS Prepaid Debit Card

DSHS is seeking the following Prepaid Debit Card services. All Prepaid Debit Card services required must be installed and fully operational on or before October 1, 2025.

The financial institution must cooperate in the transition of the Prepaid Debit Card to another financial institution if they are not awarded subsequent contract at the end of this agreement. If the financial institution chooses not to pursue a subsequent contract at the end of this agreement, they must notify DCS at least twelve (12) months prior and must cooperate with the transition of all bank services to another financial institution.

(1) The financial institution shall provide a Prepaid Debit Card program for DCS customers to have their child support deposited into reloadable individual accounts set up for each participating cardholder to access their funds.

(2) The financial institution must guarantee that the existing Prepaid Debit Card account holder information will transfer in its entirety to the successful contractor's system.

(3) Prepaid Debit Card program shall be provided at no cost to DSHS/DCS and without any account maintenance fees for cardholders.

(4) DCS shall provide sufficient information regarding each cardholder to establish an account unique to that cardholder. Cards are to be issued to cardholders by the financial institution at no

charge to DSHS/DCS or the cardholder when expedited service is not requested. DCS shall transmit funds through the ACH on a regular basis that will be loaded onto each cardholder's account.

(5) The financial institution must be able to receive at minimum, batch enrollment files via SFTP and return an "Echo" enrollment file that includes identical information that was sent by the state, card enrollment report and a rejected enrollee report that includes the reason for rejection. DCS desires to self-assign "Pay to" card account numbers that will be uniquely assigned to each customer for use throughout their enrollment in the program.

(6) The financial institution will provide secure access via the Internet for DCS staff to enroll new cardholders, update account information, and review payments applied to the accounts, as well as batch file upload capabilities or other online processes, at a minimum, requesting new cards be mailed.

(7) Card enrollees reside both domestically or abroad and will require "travel exceptions" for using their cards in foreign countries for several months at a time or for the duration of the card account.

(8) Card accounts should only be closed upon permission of DCS, unless cardholder is otherwise disqualified by the bank.

(9) The financial institution will provide a dedicated team to provide card customer service, product development, and problem resolution for DCS staff Monday through Friday between the hours of 8:00 AM and 5:30 PM PST.

(10) The financial institution must provide on-line management reports of card and staff cardholder update activity to use as an audit tool for tracking changes, at no charge to DSHS/DCS.

(11) Cardholders must be able to have free options to access funds on their account in the same way they would with a bank account debit card, including but not limited to: through ATMs, Point of Sale, Internet, telephone, teller withdrawals, On-Line Bill Pay, and other options.

(12) The financial institution must provide options for cardholders to receive monthly account statements by mail, account alerts by text or email, and mobile account access.

(13) The financial institution shall provide program transitional notifications to existing cardholders as well as periodic card program marketing materials, usage guides, and educational information at no charge to DCS. Required marketing materials include those that accompany the card and may include additional inserts or educational materials to be provided for our staff and customers or mailed with paper statements. All materials need to be approved by DCS prior to release.

(14) Contractor must provide 24 hour customer service for card holders through a toll free phone number with IVR system and secure Internet access unique to the Washington State DSHS/DCS program.

(15) Language Interpretation Services must be provided by Financial Institution for Card customers, including customers with special needs such as TeleTYpewriter/ Telecommunications Device for the Deaf (TTY/TTD) services.

(16)   The financial institution shall provide Consumer Financial Protection Bureau (CFPB) Disclosure materials, along with disclosures translated into foreign languages, and keep DCS up to date with changes to requirements.

(17)   DCS may opt out of portions of a contract that provide Prepaid Debit Card services in the event DSHS or the State Treasurer's Office procures a contract designed for all state agencies disbursing funds to recipients or other changes to state policy requiring the merging of such a program with other state agencies.

c. Additional Creative Technology and Service Solutions

This is an opportunity for Bidders to recommend the use of new and innovative technologies that will provide improved service and/or operational savings when formulating a response. The introductions of new technologies and services can occur at any time during the contract term. However, DCS shall retain approval authority in the use or employment of these new technologies.

New technologies and services could include but are not limited to:

(1) Emergency replacement of lost/stolen card at bank branch;

(2) Option to make child support payments at Bidder's branch kiosk/ATMs;

(3) Other Electronic commerce options; and/or

(4) On-line, IVR system, walk-in and/or other payment solutions.

DCS expects the selected financial institution to provide leadership and guidance in the development and implementation of new technologies related to banking services throughout the term of the Agreement.

5.   Consideration.

a. Total consideration payable to the Contractor for satisfactory performance of the work under this Contract is fee for service.

b. Any and all expenses and those costs shall be based on the rates listed in Exhibit C.

c. The Contractor will maintain reasonably up-to-date software and hardware technology at no additional cost to DCS.

d. In the event of implementation of banking services not listed in Exhibit C, all fees associated with the banking services must be pre-approved in writing by DSHS.

6.   Billing and Payment.

a. Invoice System. The Contractor shall submit a monthly Account Analysis to the DSHS Economic Services Administration, DCS Central Services at PO Box 9162, Olympia, WA 98507-9162.

Special Terms and Conditions

    b.   The Account Analysis shall describe balance, compensation and service activity for each of the Zero Balance Accounts (ZBA) and the Demand Deposit Account (DDA) to the satisfaction of DSHS. Each section of the Account Analysis shall contain, at a minimum, the following:

        (1) Service code;

        (2) Service definition;

        (3) Volume for the month;

        (4) Price for item; and

        (5) A section that, at a minimum, includes current month and year-to-date information on:

            (a) Average ledger balance;

            (b) Float;

            (c) Average collected balance;

            (d) Net collected balance;

            (e) Balance available for earnings;

            (f) Service charge detail;

            (g) Earnings credit;

            (h) Earnings rate; and

            (i) Total fees.

    c.   The Contractor shall submit an annual invoice for payment included with the June Account Analysis with the cumulative total due for the year.

    d.   The Contractor shall provide monthly Account Analysis statements that includes all the banking fees charged for services provided. The fees will accumulate from month-to-month and are payable after the end of the State Fiscal Year closing June 30th.

    e.   The Contractor shall provide DCS with the ability to submit payments made from excess earnings credit on the DCS account.

    f.   The Contractor will allow DCS to submit order/billings through the Contractor (financial institution) with payments to be made by the financial institution, from excess earnings credit on DCS account(s). Order/billings may include, but are not limited to, deposit slips, bags, endorsement plate costs, ACH/financial institution publications, and other items as deemed appropriate to be reviewed with the relationship manager for feasibility of being placed on the Account Analysis.

    g.   The Contractor shall carry over any earnings credits on the monthly Account Analysis statement reconciled at the end of the State Fiscal year end during the Period of Performance of this Contract.

    h.   Payment shall be considered timely if made by DSHS within thirty (30) days after receipt and

acceptance of properly completed invoices. Payment shall be sent to the address designated by the Contractor on the invoice received with the Account Analysis Statement. DSHS, may, at its sole discretion, withhold payment claimed by the Contractor for services rendered if Contractor fails to satisfactorily comply with any term or condition of this Contract.

7.   Disputes.

Either party may submit a request for resolution of a contract dispute (rates set by law, regulation or DSHS policy are not disputable). The requesting party shall submit a written statement identifying the issue(s) in dispute and the relative positions of the parties. A request for a dispute resolution must include the Contractor's name, address, and contract number, and be mailed to the address listed below within thirsty (30) calendar days after the party could reasonably be expected to have knowledge of the issue in dispute.

> DSHS/ESA/Division of Child Support (DCS)
>
> P.O. Box 9162
>
> Olympia, WA 98507-9162
>
> Attn. DCS Contracts Unit

8.   Data Sharing

a.   Description of Data

   (1) The data shall only be used by the Contractor for the purpose of administering the DCS child support government banking account.

   (2) The following client information may be provided to the Contractor:

   (a) Name;

   (b) Address;

   (c) Telephone number;

   (d) Mother's maiden name;

   (e) DCS case number;

   (f) Social Security number;

   (g) Unique Agency Identification number; and

   (h) Bank account number.

b.   Access to Data

   (1) Method of Access

Special Terms and Conditions

        (a) DCS will transmit electronic data using a secure file transfer protocol (SFTP).

c. Persons Having Access to Data

    (1) Access to data shall be limited to the authorized Contractor's staff whose duties specifically require access to the data in the performance of their assigned duties.

    (2) The Contractor shall store the data on a network share which uses access control lists to ensure that only authorized users can access the data through workstations. A unique logon ID and complex password are required to loon to the network and access the data.

    (3) All of Contractor's staff who have access to DCS data shall sign the Non-DCS Employee Confidentiality Agreement, Exhibit C.

d. Frequency of Data Exchange

    (1) Daily

e. Unauthorized Disclosure of Data

    (1) The Contractor shall within twelve (12) hours of the Contractor's relationship manager or designee becoming aware of an unauthorized disclosure of data referenced above, notify the DSHS Contact listed on page one (1) or designee.

Special Terms and Conditions

Exhibit A – Data Security Requirements

1. **Definitions**. The words and phrases listed below, as used in this Exhibit, shall each have the following definitions:

    a. "AES" means the Advanced Encryption Standard, a specification of Federal Information Processing Standards Publications for the encryption of electronic data issued by the National Institute of Standards and Technology (http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf).

    b. "Authorized Users(s)" means an individual or individuals with a business need to access DSHS Confidential Information, and who has or have been authorized to do so.

    c. "Business Associate Agreement" means an agreement between DSHS and a contractor who is receiving Data covered under the Privacy and Security Rules of the Health Insurance Portability and Accountability Act of 1996. The agreement establishes permitted and required uses and disclosures of protected health information (PHI) in accordance with HIPAA requirements and provides obligations for business associates to safeguard the information.

    d. "Category 4 Data" is data that is confidential and requires special handling due to statutes or regulations that require especially strict protection of the data and from which especially serious consequences may arise in the event of any compromise of such data. Data classified as Category 4 includes but is not limited to data protected by: the Health Insurance Portability and Accountability Act (HIPAA), Pub. L. 104-191 as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH), 45 CFR Parts 160 and 164; the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. §1232g; 34 CFR Part 99; Internal Revenue Service Publication 1075 (https://www.irs.gov/pub/irs-pdf/p1075.pdf); Substance Abuse and Mental Health Services Administration regulations on Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR Part 2; and/or Criminal Justice Information Services, 28 CFR Part 20.

    e. "Cloud" means data storage on servers hosted by an entity other than the Contractor and on a network outside the control of the Contractor. Physical storage of data in the cloud typically spans multiple servers and often multiple locations. Cloud storage can be divided between consumer grade storage for personal files and enterprise grade for companies and governmental entities. Examples of consumer grade storage would include iTunes, Dropbox, Box.com, and many other entities. Enterprise cloud vendors include Microsoft Azure, Amazon Web Services, and Rackspace.

    f. "Encrypt" means to encode Confidential Information into a format that can only be read by those possessing a "key"; a password, digital certificate or other mechanism available only to authorized users. Encryption must use a key length of at least 256 bits for symmetric keys, or 2048 bits for asymmetric keys. When a symmetric key is used, the Advanced Encryption Standard (AES) must be used if available.

    g. "FedRAMP" means the Federal Risk and Authorization Management Program (see www.fedramp.gov), which is an assessment and authorization process that federal government agencies have been directed to use to ensure security is in place when accessing Cloud computing products and services.

    h. "Hardened Password" means a string of at least eight characters containing at least three of the following four character classes: Uppercase alphabetic, lowercase alphabetic, numeral, and special characters such as an asterisk, ampersand, or exclamation point.

i.   "Mobile Device" means a computing device, typically smaller than a notebook, which runs a mobile operating system, such as iOS, Android, or Windows Phone. Mobile Devices include smart phones, most tablets, and other form factors.

j.   "Multi-factor Authentication" means controlling access to computers and other IT resources by requiring two or more pieces of evidence that the user is who they claim to be. These pieces of evidence consist of something the user knows, such as a password or PIN; something the user has such as a key card, smart card, or physical token; and something the user is, a biometric identifier such as a fingerprint, facial scan, or retinal scan. "PIN" means a personal identification number, a series of numbers which act as a password for a device. Since PINs are typically only four to six characters, PINs are usually used in conjunction with another factor of authentication, such as a fingerprint.

k.   "Portable Device" means any computing device with a small form factor, designed to be transported from place to place. Portable devices are primarily battery powered devices with base computing resources in the form of a processor, memory, storage, and network access. Examples include, but are not limited to, mobile phones, tablets, and laptops. Mobile Device is a subset of Portable Device.

l.   "Portable Media" means any machine readable media that may routinely be stored or moved independently of computing devices. Examples include magnetic tapes, optical discs (CDs or DVDs), flash memory (thumb drive) devices, external hard drives, and internal hard drives that have been removed from a computing device.

m.   "Secure Area" means an area to which only authorized representatives of the entity possessing the Confidential Information have access, and access is controlled through use of a key, card key, combination lock, or comparable mechanism. Secure Areas may include buildings, rooms or locked storage containers (such as a filing cabinet or desk drawer) within a room, as long as access to the Confidential Information is not available to unauthorized personnel. In otherwise Secure Areas, such as an office with restricted access, the Data must be secured in such a way as to prevent access by non-authorized staff such as janitorial or facility security staff, when authorized Contractor staff are not present to ensure that non-authorized staff cannot access it.

n.   "Trusted Network" means a network operated and maintained by the Contractor, which includes security controls sufficient to protect DSHS Data on that network. Controls would include a firewall between any other networks, access control lists on networking devices such as routers and switches, and other such mechanisms which protect the confidentiality, integrity, and availability of the Data.

o.   "Unique User ID" means a string of characters that identifies a specific user and which, in conjunction with a password, passphrase or other mechanism, authenticates a user to an information system.

2.   **Authority**. The security requirements described in this document reflect the applicable requirements of Standard 141.10 (https://ocio.wa.gov/policies) of the Office of the Chief Information Officer for the state of Washington, and of the DSHS Information Security Policy and Standards Manual. Reference material related to these requirements can be found here: https://www.dshs.wa.gov/ffa/keeping-dshs-client-information-private-and-secure, which is a site developed by the DSHS Information Security Office and hosted by DSHS Central Contracts and Legal Services.

3.   **Administrative Controls.** The Contractor must have the following controls in place:

a. A documented security policy governing the secure use of its computer network and systems, and which defines sanctions that may be applied to Contractor staff for violating that policy.

b. If the Data shared under this agreement is classified as Category 4, the Contractor must be aware of and compliant with the applicable legal or regulatory requirements for that Category 4 Data.

c. If Confidential Information shared under this agreement is classified as Category 4, the Contractor must have a documented risk assessment for the system(s) housing the Category 4 Data.

4. **Authorization, Authentication, and Access.** In order to ensure that access to the Data is limited to authorized staff, the Contractor must:

a. Have documented policies and procedures governing access to systems with the shared Data.

b. Restrict access through administrative, physical, and technical controls to authorized staff.

c. Ensure that user accounts are unique and that any given user account logon ID and password combination is known only to the one employee to whom that account is assigned. For purposes of non-repudiation, it must always be possible to determine which employee performed a given action on a system housing the Data based solely on the logon ID used to perform the action.

d. Ensure that only authorized users are capable of accessing the Data.

e. Ensure that an employee's access to the Data is removed immediately:

(1) Upon suspected compromise of the user credentials.

(2) When their employment, or the contract under which the Data is made available to them, is terminated.

(3) When they no longer need access to the Data to fulfill the requirements of the contract.

f. Have a process to periodically review and verify that only authorized users have access to systems containing DSHS Confidential Information.

g. When accessing the Data from within the Contractor's network (the Data stays within the Contractor's network at all times), enforce password and logon requirements for users within the Contractor's network, including:

(1) A minimum length of 8 characters, and containing at least three of the following character classes: uppercase letters, lowercase letters, numerals, and special characters such as an asterisk, ampersand, or exclamation point.

(2) That a password does not contain a user's name, logon ID, or any form of their full name.

(3) That a password does not consist of a single dictionary word. A password may be formed as a passphrase which consists of multiple dictionary words.

(4) That passwords are significantly different from the previous four passwords. Passwords that increment by simply adding a number are not considered significantly different.

h. When accessing Confidential Information from an external location (the Data will traverse the Internet or otherwise travel outside the Contractor's network), mitigate risk and enforce password and logon requirements for users by employing measures including:

(1) Ensuring mitigations applied to the system don't allow end-user modification.

(2) Not allowing the use of dial-up connections.

(3) Using industry standard protocols and solutions for remote access. Examples would include RADIUS and Citrix.

(4) Encrypting all remote access traffic from the external workstation to Trusted Network or to a component within the Trusted Network. The traffic must be encrypted at all times while traversing any network, including the Internet, which is not a Trusted Network.

(5) Ensuring that the remote access system prompts for re-authentication or performs automated session termination after no more than 30 minutes of inactivity.

(6) Ensuring use of Multi-factor Authentication to connect from the external end point to the internal end point.

i. Passwords or PIN codes may meet a lesser standard if used in conjunction with another authentication mechanism, such as a biometric (fingerprint, face recognition, iris scan) or token (software, hardware, smart card, etc.) in that case:

(1) The PIN or password must be at least 5 letters or numbers when used in conjunction with at least one other authentication factor

(2) Must not be comprised of all the same letter or number (11111, 22222, aaaaa, would not be acceptable)

(3) Must not contain a "run" of three or more consecutive numbers (12398, 98743 would not be acceptable)

j. If the contract specifically allows for the storage of Confidential Information on a Mobile Device, passcodes used on the device must:

(1) Be a minimum of six alphanumeric characters.

(2) Contain at least three unique character classes (upper case, lower case, letter, number).

(3) Not contain more than a three consecutive character run. Passcodes consisting of 12345, or abcd12 would not be acceptable.

k. Render the device unusable after a maximum of 10 failed logon attempts.

5. **Protection of Data**. The Contractor agrees to store Data on one or more of the following media and protect the Data as described:

a. **Hard disk drives**. For Data stored on local workstation hard disks, access to the Data will be restricted to Authorized User(s) by requiring logon to the local workstation using a Unique User ID

and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards.

b. **Network server disks**. For Data stored on hard disks mounted on network servers and made available through shared folders, access to the Data will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has authenticated to the network using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on disks mounted to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

For DSHS Confidential Information stored on these disks, deleting unneeded Data is sufficient as long as the disks remain in a Secure Area and otherwise meet the requirements listed in the above paragraph. Destruction of the Data, as outlined below in Section 8 Data Disposition, may be deferred until the disks are retired, replaced, or otherwise taken out of the Secure Area.

c. **Optical discs (CDs or DVDs) in local workstation optical disc drives**. Data provided by DSHS on optical discs which will be used in local workstation optical disc drives and which will not be transported out of a Secure Area. When not in use for the contracted purpose, such discs must be Stored in a Secure Area. Workstations which access DSHS Data on optical discs must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

d. **Optical discs (CDs or DVDs) in drives or jukeboxes attached to servers**. Data provided by DSHS on optical discs which will be attached to network servers and which will not be transported out of a Secure Area. Access to Data on these discs will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has authenticated to the network using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on discs attached to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

e. **Paper documents**. Any paper records must be protected by storing the records in a Secure Area which is only accessible to authorized personnel. When not in use, such records must be stored in a Secure Area.

f. **Remote Access**. Access to and use of the Data over the State Governmental Network (SGN) or Secure Access Washington (SAW) will be controlled by DSHS staff who will issue authentication credentials (e.g. a Unique User ID and Hardened Password) to Authorized Users on Contractor's staff. Contractor will notify DSHS staff immediately whenever an Authorized User in possession of such credentials is terminated or otherwise leaves the employ of the Contractor, and whenever an Authorized User's duties change such that the Authorized User no longer requires access to perform work for this Contract.

g. **Data storage on portable devices or media**.

(1) Except where otherwise specified herein, DSHS Data shall not be stored by the Contractor on portable devices or media unless specifically authorized within the terms and conditions of the Contract. If so authorized, the Data shall be given the following protections:

(a) Encrypt the Data.

(b) Control access to devices with a Unique User ID and Hardened Password or stronger authentication method such as a physical token or biometrics.

(c) Manually lock devices whenever they are left unattended and set devices to lock automatically after a period of inactivity, if this feature is available. Maximum period of inactivity is 20 minutes.

(d) Apply administrative and physical security controls to Portable Devices and Portable Media by:

    i. Keeping them in a Secure Area when not in use,

    ii. Using check-in/check-out procedures when they are shared, and

    iii. Taking frequent inventories.

(2) When being transported outside of a Secure Area, Portable Devices and Portable Media with DSHS Confidential Information must be under the physical control of Contractor staff with authorization to access the Data, even if the Data is encrypted.

h. **Data stored for backup purposes**.

(1) DSHS Confidential Information may be stored on Portable Media as part of a Contractor's existing, documented backup process for business continuity or disaster recovery purposes. Such storage is authorized until such time as that media would be reused during the course of normal backup operations. If backup media is retired while DSHS Confidential Information still exists upon it, such media will be destroyed at that time in accordance with the disposition requirements below in Section 8 *Data Disposition*.

(2) Data may be stored on non-portable media (e.g. Storage Area Network drives, virtual media, etc.) as part of a Contractor's existing, documented backup process for business continuity or disaster recovery purposes. If so, such media will be protected as otherwise described in this exhibit. If this media is retired while DSHS Confidential Information still exists upon it, the data will be destroyed at that time in accordance with the disposition requirements below in Section 8 *Data Disposition*.

i. **Cloud storage**. DSHS Confidential Information requires protections equal to or greater than those specified elsewhere within this exhibit. Cloud storage of Data is problematic as neither DSHS nor the Contractor has control of the environment in which the Data is stored. For this reason:

(1) DSHS Data will not be stored in any consumer grade Cloud solution, unless all of the following conditions are met:

    (a) Contractor has written procedures in place governing use of the Cloud storage and Contractor attests in writing that all such procedures will be uniformly followed.

    (b) The Data will be Encrypted while within the Contractor network.

    (c) The Data will remain Encrypted during transmission to the Cloud.

(d) The Data will remain Encrypted at all times while residing within the Cloud storage solution.

(e) The Contractor will possess a decryption key for the Data, and the decryption key will be possessed only by the Contractor and/or DSHS.

(f) The Data will not be downloaded to non-authorized systems, meaning systems that are not on either the DSHS or Contractor networks.

(g) The Data will not be decrypted until downloaded onto a computer within the control of an Authorized User and within either the DSHS or Contractor's network.

(2) Data will not be stored on an Enterprise Cloud storage solution unless either:

(a) The Cloud storage provider is treated as any other Sub-Contractor, and agrees in writing to all of the requirements within this exhibit; or,

(b) The Cloud storage solution used is FedRAMP certified.

(3) If the Data includes protected health information covered by the Health Insurance Portability and Accountability Act (HIPAA), the Cloud provider must sign a Business Associate Agreement prior to Data being stored in their Cloud solution.

6. **System Protection**. To prevent compromise of systems which contain DSHS Data or through which that Data passes:

   a. Systems containing DSHS Data must have all security patches or hotfixes applied within 3 months of being made available.

   b. The Contractor will have a method of ensuring that the requisite patches and hotfixes have been applied within the required timeframes.

   c. Systems containing DSHS Data shall have an Anti-Malware application, if available, installed.

   d. Anti-Malware software shall be kept up to date. The product, its anti-virus engine, and any malware database the system uses, will be no more than one update behind current.

7. **Data Segregation**.

   a. DSHS Data must be segregated or otherwise distinguishable from non-DSHS data. This is to ensure that when no longer needed by the Contractor, all DSHS Data can be identified for return or destruction. It also aids in determining whether DSHS Data has or may have been compromised in the event of a security breach. As such, one or more of the following methods will be used for data segregation.

   (1) DSHS Data will be kept on media (e.g. hard disk, optical disc, tape, etc.) which will contain no non-DSHS Data. And/or,

   (2) DSHS Data will be stored in a logical container on electronic media, such as a partition or folder dedicated to DSHS Data. And/or,

   (3) DSHS Data will be stored in a database which will contain no non-DSHS data. And/or,

      (4) DSHS Data will be stored within a database and will be distinguishable from non-DSHS data by the value of a specific field or fields within database records.

      (5) When stored as physical paper documents, DSHS Data will be physically segregated from non-DSHS data in a drawer, folder, or other container.

   b. When it is not feasible or practical to segregate DSHS Data from non-DSHS data, then both the DSHS Data and the non-DSHS data with which it is commingled must be protected as described in this exhibit.

8.   **Data Disposition**. When the contracted work has been completed or when the Data is no longer needed, except as noted above in Section 5.b, Data shall be returned to DSHS or destroyed. Media on which Data may be stored and associated acceptable methods of destruction are as follows:

Data stored on:	Will be destroyed by:
Server or workstation hard disks, or Removable media (e.g. floppies, USB flash drives, portable hard disks) excluding optical discs	Using a "wipe" utility which will overwrite the Data at least three (3) times using either random or single character data, or Degaussing sufficiently to ensure that the Data cannot be reconstructed, or Physically destroying the disk
Paper documents with sensitive or Confidential Information	Recycling through a contracted firm, provided the contract with the recycler assures that the confidentiality of Data will be protected.
Paper documents containing Confidential Information requiring special handling (e.g. protected health information)	On-site shredding, pulping, or incineration
Optical discs (e.g. CDs or DVDs)	Incineration, shredding, or completely defacing the readable surface with a coarse abrasive
Magnetic tape	Degaussing, incinerating or crosscut shredding

9.   **Notification of Compromise or Potential Compromise**. The compromise or potential compromise of DSHS shared Data must be reported to the DSHS Contact designated in the Contract within one (1) business day of discovery. If no DSHS Contact is designated in the Contract, then the notification must be reported to the DSHS Privacy Officer at dshsprivacyofficer@dshs.wa.gov. Contractor must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law or DSHS.

10.   **Data shared with Subcontractors**. If DSHS Data provided under this Contract is to be shared with a subcontractor, the Contract with the subcontractor must include all of the data security provisions within this Contract and within any amendments, attachments, or exhibits within this Contract. If the Contractor cannot protect the Data as articulated within this Contract, then the contract with the sub-Contractor must be submitted to the DSHS Contact specified for this contract for review and approval.