State of Washington
Department of Corrections

Contract No. [INSERT #]

This Contract is entered into by and between the Washington State Department of Corrections, hereinafter referred to as "Department" or "DOC," [INSERT CONTRACTOR], located at [INSERT PRIMARY CONTRACTOR ADDRESS] and hereinafter referred to as "Contractor," for the express purposes set forth in the following provisions of this Contract. The Department and Contractor may be collectively referred to as the "Parties" or individually as a "Party."

WHEREAS the purpose of this Contract is to secure the expert services of independent contractors whose expertise is required by DOC.

WHEREAS this is a competitively procured purchase in compliance with RCW 39.26.102.

NOW THEREFORE, in consideration of the terms and conditions contained herein, or attached and incorporated and made a part hereof, the Department and Contractor agree as follows:

I. CONTRACT TERM

Subject to other Contract provisions, the term under this Contract will be from MONTH DAY, YEAR through MONTH DAY, YEAR, or until DOC in its sole authority decides it is in the best interest of DOC to terminate the agreement upon one (1) month's written notice.

DOC and Contractor may extend the contract for an additional one (1) year term by written amendment by the Parties.

II. RIGHTS AND OBLIGATIONS

All rights and obligations of the Parties to this Contract shall be subject to and governed by the special terms and conditions contained in the text of this Contract instrument, the General Terms and Conditions attached hereto as Attachment A, and the Statement of Work [OPTIONAL] attached hereto as Attachment B. [ADD ANY VENDOR ATTACHEMNTS]

III. COMPENSATION AND PAYMENT

Total consideration payable to Contractor for satisfactory performance of the work under this Contract is contingent and based upon the rates of the apparent successful bidder(s) under ITPS Work Request #

Contractors may biannually adjust their Contractor hourly rate(s) based upon the U.S. Bureau of Labor Statistics published Consumer Price Index for the preceding two years to keep pricing competitive under this Agreeement. Consumer Price Index information is available at: https://www.bls.gov/cpi/

[INSERT BID RATES]

A. Compensation is contingent upon Contractor meeting the performance standards and attaining the outcome measures for the contracted services that are detailed in the Statement of Work, Attachment B. Any additional services provided by the Contractor must have the prior written approval of the Department.

B. Time of Payment. Payment shall be considered timely if made by the Department within 30 days after receipt of properly completed invoices. Payment shall be sent to the address designated by the Contractor. The Department may, at its sole discretion, terminate the Contract or withhold payments claimed by the Contractor for services rendered if the Contractor fails to satisfactorily comply with any term or condition of this Contract.

C. Method of Payment. Compensation for services rendered shall be payable upon submittal of properly completed invoices. The Contractor shall submit invoices to the Contract Manager together with a detailed statement of the Contract services performed for which the Contractor is seeking compensation.

D. Invoices Required. Requests for payment under this Contract shall be submitted by the Contractor on Invoices (State Form A-19) prepared in the manner prescribed by the Department. These invoices shall include such information as is necessary for the Department to determine the exact nature of all expenditures. Each invoice will clearly indicate that it is for the services rendered in performance under this Contract.

IV. INSURANCE

A. Contractor shall maintain insurance coverage in full force and effect during the entire term of this Contract as set out below. The insurance required shall be issued by an insurance company authorized to do business within the state of Washington, and shall name the state of Washington, its agents and employees as additional insureds. All policies shall be primary to any other valid and collectable insurance. Contractor shall notify the Department in writing thirty (30) days prior to any material alteration, cancellation, or replacement of an existing policy. Contractor shall instruct the insurers to give the Department thirty (30) days advance notice of any cancellation of an existing policy.

B. Professional Liability: Contractor shall maintain professional liability insurance during the term of this Contract, including coverage for losses caused by errors or omissions. Such policy shall contain the following limits: Each occurrence - $1,000,000; General Aggregate - $2,000,000.

C. Commercial Form General Liability Insurance (contractual liability included) with minimum limits of $2,000,000.00 for each occurrence and $4,000,000.00 for general aggregate. If the insurance is written on a claims-made form, it shall continue for three (3) years following termination of this Contract. The insurance shall have a retroactive date of placement prior to or coinciding with the commencement of the Term of this Contract

D. In the event that services delivered pursuant to this Contract involve the use of vehicles, either owned or unowned by the Contractor, Contractor shall maintain business auto liability and, if necessary, commercial umbrella liability insurance with a limit not less than $1,000,000 per accident.

E. The Contractor will at all times comply with all applicable workers' compensation, occupational disease, and occupational health and safety laws, statutes, and regulations to the full extent applicable. The State will not be held responsible in any way for claims filed by the Contractor or their employees for services performed under the terms of this Contract.

F. Contractor will provide the Department with one copy of the certificate of insurance for each coverage required under the Contract. Each copy will contain the contract number to which it applies at the top and shall be sent to the Contracts and Legal Affairs Section at docclacontracts@doc1.wa.gov. Contractor shall immediately notify the Contracts and Legal Affairs Section in the event such policy is terminated, canceled, or modified.

V. CONTRACT REPRESENTATIVES

A. The Department's Contract Manager for this Contract shall be _____ (_____doc1.wa.gov). The Contract Manager shall be responsible for monitoring the performance of the Contractor, the approval of actions by the Contractor, approval for payment of billings and expenses submitted by the Contractor, and the acceptance of any reports by the Contractor.

B. The Contractor's representative for this Contract shall be _____, who will be contact person for all communications regarding the conduct of work under this Contract.

VI. INDEPENDENT CONTRACTOR STATUS

The Contractor is not an employee of the Department of Corrections. By signing this Contract, the Contractor certifies that he or she is not a current Department employee, and will advise the Department immediately should this status change. This Contract shall become null and void if the Contractor accepts employment with the Department. The Contractor shall not hold himself out as nor claim to be an officer or employee of the State of Washington by reason hereof. The Contractor agrees not to make any claim, demand, or application to or for any right or privilege applicable to a Department employee or state of Washington employee including but not limited to, workmen's compensation coverage or retirement membership or credit or any other benefit which would accrue to a civil service employee.

VII. INDEPENDENT CONTRACTOR PROVISIONS

DOC expects any possible awarded Contractor to make best efforts to provide the staff submitted in their original bid throughout the life of the Contract. Should individuals become unavailable between the time of Bidder submitting their bid and being selected for an award, DOC may at DOC's sole discretion, accept substitute personnel with comparable experience at the same hourly rate or a lessor hourly rate. DOC understands that supplied contractors may become unavailable during the lifespan of any possible Contract and may request Contractor proposals of similarly experienced individuals submitted to continue performance under the Contract.

DOC reserves the right to report substandard performance to Contractor and to require Contractor submission of substitute personnel in the event that performance issues cannot be remedied with reasonable efforts on the part of DOC and Contractor.

DOC is seeking to fill the positions bid for in the RF_____ _____ Attachment D Bidder Response document. However, these needs may change during the term of the contract via an increase or decrease in the personnel needs of DOC. Thus, DOC reserves the right to request additional staff to fill more positions aligning with the Java Developer, Software Tester, or Business Analyst categories respectively. These additional positions, if needed, would be able to be filled by written amendment with a possible awarded Contractor and would not exceed the highest hourly rate bid under the bidders RFQQ 12815 Attachment D response for that position category.

Should DOC's needs decrease during the term of the Work Order/Scope of Work, DOC may give Contractor one (1) months' notice that specified Work Order personnel are no longer necessary and reduce services accordingly.

VIII. INTERPRETATION OF CONTRACT

A. Order of Precedence. In the event of an inconsistency in this Contract, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order:

- Applicable federal and state of Washington statutes and regulations
- Special terms and conditions contained in this basic Contract instrument
- Any other provision, term, or material incorporated herein by reference or otherwise incorporated

B. Entire Agreement. This Contract including referenced schedules represents all the terms and conditions agreed upon by the Parties. No other understanding or representations, oral or otherwise, regarding the subject matter of this Contract shall be deemed to exist or to bind any of the Parties hereto.

C. Conformance. If any provision of this Contract violates any statute or rule of law of the state of Washington, it is considered modified to conform to that statute or rule of law.

D. Counterparts. This Contract may be executed in duplicate originals and, for all purposes, each duplicate shall be deemed an original copy of the Contract signed by each Party.

E. Approval. This Contract shall be subject to the written approval of the Department's authorized representative and shall not be binding until so approved. The Contract may be altered, amended, or waived only by a written amendment executed by both Parties.

THIS CONTRACT, is executed by the persons signing below who warrant that they have the authority to execute the Contract.

[INSERT CONTRACTOR LEGAL NAME]	**DEPARTMENT OF CORRECTIONS**
(Signature)	(Signature)
(Printed Name)	Daryl A. Huntsinger (Printed Name)
(Title)	Contracts Administrator (Title)
(Date)	(Date)

Approved as to Form: This Contract format was approved by the Office of the Attorney General. Approval on file.

ATTACHMENT A – GENERAL TERMS AND CONDITIONS

WASHINGTON STATE
DEPARTMENT OF CORRECTIONS

1. DEFINITIONS

As used throughout this Contract, the following terms shall have the meanings set forth below:

1.1 "Contractor" shall mean 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. "Contractor" shall also include any Subcontractor retained by the Contractor as permitted under the terms of this Contract.

1.2 "Secretary" shall mean the Secretary of the Department of Corrections and designees authorized to act on the Secretary's behalf.

1.3 "Department" shall mean the Department of Corrections (DOC) of the state of Washington, any division, section, office, unit or other sub-division of the Department, or any of the officers or other officials lawfully representing the Department.

1.4 "Subcontractor" shall mean one not in the employment of the Contractor who, under a separate contract with the Contractor, is performing all or part of the services under this Contract. Contractor shall remain responsible to the Department for any work required under the terms of this contract that is performed by a subcontractor under separate contract to Contractor.

1.5 "Contracts Administrator" shall mean the Administrator of Contracts and Legal Affairs or designee.

1.6 "Contracts and Legal Affairs" shall mean the Department of Corrections (DOC) headquarters contracting office, or successor section or office.

1.7 "Individual" and "Individuals" shall mean person or persons under the jurisdiction of the Department of Corrections.

2. ACCESS TO DATA

The Contractor shall, at no additional cost, provide access to data generated under this Contract to the Department, the Washington State Joint Legislative Audit and Review Committee, and the Washington State Auditor. This includes access to all information that supports the findings, conclusions, and recommendations of the Contractor's reports, including computer models and methodology for those models.

3. AMERICANS WITH DISABILITIES ACT (ADA)

The Contractor must comply with the ADA, which provides comprehensive civil rights protection to individuals with disabilities in the areas of employment, public accommodations, state and local government services, and telecommunications. (See Americans with Disabilities Act (ADA) of 1990, Public Law 101-336, also referred to as the "ADA" 28 CFR Part 35.)

4. ADVANCE PAYMENTS PROHIBITED

No payments in advance of or in anticipation of goods or services to be provided under this contract shall be made by the Department.

5. AMENDMENTS AND MODIFICATIONS

5.1 Amendments and modifications to this contract shall not be binding unless they are in writing and signed by personnel authorized to bind each of the parties.

5.2 Changes in the rate of compensation must be signed by both parties and shall not be effective until the first day of the month following the last date of signature of the amendment or until the effective date of the amendment if later than the date of last signature.

5.3 The Secretary may, at any time, by written notification to the Contractor, and without notice to any guarantor or surety, unilaterally amend the scope of work to be performed under the Contract, the period of performance, or the compensation to be paid to the Contractor. These unilateral changes shall be effective as set forth in the amendment or upon signature by the Contracts Administrator, if no date has been set forth.

5.4 The Contractor will be deemed to have accepted any such unilateral amendment unless, within fifteen (15) calendar days after the date the amendment is signed by the Contracts Administrator, the Contractor notifies the Contract Manager, in writing, of its non-acceptance of such unilateral change. The Contractor and the Department will then use good faith efforts to negotiate an amendment acceptable to both parties.

5.5 Failure to reach agreement shall constitute a dispute concerning a question of fact within the meaning of the Disputes provision contained in this Contract. However, nothing in this provision shall excuse the Contractor from proceeding with the Contract as amended. Contractor must continue to provide the contracted services, including any unilaterally amended services, during any period of non-acceptance or negotiation of a unilateral amendment.

6. ASSIGNMENT

Neither this contract, nor any claim arising under this contract, shall be transferred or assigned by the Contractor without prior written consent of the Department.

7. ATTORNEYS' FEES

In the event of litigation or other action brought to enforce contract terms, each party agrees to bear its own attorney fees and costs.

8. CONFIDENTIALITY/SAFEGUARDING OF INFORMATION

8.1 "Confidential Information" as used in this section includes:

8.1.1. All material provided to the Contractor by the Department that is designated as "confidential" by the Department;

8.1.2. All material produced by the Contractor that is designated as "confidential" by the Department; and

8.1.3. All personal information in the possession of the Contractor that may not be disclosed under state or federal law. "Personal information" includes but is not limited to information related to a person's name, health, finances, education, business, use of government services, addresses, telephone numbers, social security number, driver's license number and other identifying numbers, and "Protected Health Information" under the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA).

8.2 The Contractor shall comply with all state and federal laws related to the use, sharing, transfer, sale, or disclosure of Confidential Information. The Contractor shall use Confidential Information solely for the purposes of this Contract and shall not use, share, transfer, sell or disclose any Confidential Information to any third party except with the prior written consent of the Department or as may be required by law. The Contractor shall take all necessary steps to assure that Confidential Information is safeguarded to prevent unauthorized use, sharing, transfer, sale or disclosure of Confidential Information or violation of any state or federal laws related thereto. Upon request, the Contractor shall provide the Department with its policies and procedures on confidentiality. The Department may require changes to such policies and procedures as they apply to this Contract whenever the Department reasonably determines that changes are necessary to prevent unauthorized disclosures. The Contractor shall make the changes within the time period specified by the Department. Upon request, the Contractor shall immediately return to the Department any Confidential Information that the Department reasonably determines has not been adequately protected by the Contractor against unauthorized disclosure.

9. CONFLICT OF INTEREST/ETHICS

9.1 Notwithstanding any determination by the Executive Ethics Board or other tribunal, the Department may, in its sole discretion, by written notice to the Contractor, terminate this Contract if it is found after due notice and examination by the Contracts Administrator that there is a violation of the Ethics in Public Service Act, Chapter 42.52 RCW; or any similar statute involving the Contractor in the procurement of or performance under this Contract.

9.2 In the event this Contract is terminated as provided above, the Department shall be entitled to pursue the same remedies against the Contractor as it could pursue in the event of a breach of the Contract by the Contractor. The rights and remedies of the Department provided for in this clause shall not be exclusive and are in addition to any other rights and remedies provided by law. The existence of facts upon which the Contracts Administrator makes any determination under this clause shall be an issue and may be reviewed as provided in the "Disputes" clause of this Contract.

10. CONSTRUCTION

Nothing in this Contract shall be construed to create a right enforceable by or in favor of any third party.

11. COPYRIGHT PROVISIONS

11.1 Unless otherwise provided, all materials produced under this Contract shall be considered "works for hire" as defined by the U.S. Copyright Act and shall be owned by the Department. The Department shall be considered the author of such materials. In the event the materials are not considered "works for hire" under the U.S. Copyright laws, Contractor hereby irrevocably assigns all right, title, and interest in materials, including all intellectual property rights, to the Department effective from the moment of creation of such materials.

11.2 Materials means all items in any format and includes, but is not limited to, data, reports, documents, pamphlets, advertisements, books, magazines, surveys, studies, computer programs, films, tapes, and/or sound reproductions. Ownership includes the right to copyright, patent, register and the ability to transfer these rights.

11.3 For materials that are delivered under the Contract, but that incorporate pre-existing materials not produced under the Contract, Contractor hereby grants to the Department a nonexclusive, royalty-free, irrevocable license (with rights to sublicense others) in such materials to translate, reproduce,

distribute, prepare derivative works, publicly perform, and publicly display. The Contractor warrants and represents that Contractor has all rights and permissions, including intellectual property rights, moral rights and rights of publicity, necessary to grant such a license to the Department.

11.4 The Contractor shall use all reasonable effort to advise the Department, at the time of delivery of materials furnished under this Contract, of all known or potential invasions of privacy contained therein and of any portion of such document that was not produced in the performance of this Contract.

11.5 The Department shall receive prompt written notice of each notice or claim of infringement received by the Contractor with respect to any data delivered under this Contract. The Department shall have the right to modify or remove any restrictive markings placed upon the data by the Contractor.

12. COVENANT AGAINST CONTINGENT FEES

12.1 The Contractor warrants that no person or selling agency has been employed or retained to solicit or secure this Contract upon an agreement or understanding for a commission, percentage, brokerage, or contingent fee, excepting bona fide employees or bona fide established agents maintained by the Contractor for the purpose of securing business.

12.2 The Department shall have the right, in the event of breach of this clause by the Contractor, to annul this Contract without liability or, in its discretion, to deduct from the contract price or consideration or recover by other means the full amount of such commission, percentage, brokerage, or contingent fee. The provisions of this section shall survive any termination or the expiration of this Contract.

13. DISPUTES

In the event that a dispute arises under this Agreement, it shall be determined by a Dispute Board in the following manner: Each party to this Agreement shall appoint one member to the Dispute Board. The members so appointed shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall review the facts, Agreement terms and applicable statutes and rules and make a determination of the dispute. The Dispute Board shall thereafter decide the dispute with the majority prevailing.

14. DISALLOWED CHARGES/DUPLICATE CHARGES/OVERPAYMENT REFUNDS

14.1 The Contractor is not allowed to charge the Department for a Medicaid service. If the Department has erroneously paid for a Medicaid service charged by the Contractor, that payment is considered an overpayment and shall be deducted from the Contractor's future payments by the Department.

14.2 The Contractor warrants that the cost charged for services under the terms of this Contract are not in excess of the cost charged to other entities for the same service(s) nor are they a duplicate payment. If the charges are determined to be in excess of those costs charged to other entities or a duplicate charge, the Department is entitled to an overpayment refund for the excess or duplicate charges.

15. ENTIRE AGREEMENT

This Contract, all attachments, and future amendments hereto, constitute the entire agreement between the Contractor and the Department and no other statements or representations, written or oral, shall be deemed a part hereof.

16. FEDERAL IMMIGRATION REFORM AND CONTROL ACT (IRCA)

During the performance of this Contract, the Contractor shall comply with all requirements of the federal Immigration Reform and Control Act (IRCA) and any regulations adopted by the Department of Justice Bureau of Immigration and Naturalization Services to implement the IRCA. The provisions of this paragraph shall be in addition to any other requirements set forth in the text of the Contract.

17. GOVERNING LAW

This contract shall be construed and interpreted according to the laws of the state of Washington, and the venue of any action brought hereunder shall be in the Superior Court for Thurston County.

18. HEALTH and SAFETY

18.1 Health. The Contractor shall ensure that all of its personnel assigned to DOC sites is trained in the requirements of Chapter 296-823 WAC, blood borne pathogens. Further, the Contractor shall provide all such personnel with protections from blood borne and other body fluid diseases that meet or exceed the WAC standards for such protection. If the Contractor is a health care provider whose duties include the medical or physical care of Individuals or emergency or medical treatment of employees, the Contractor shall abide by the requirements of Chapter 296-823 WAC as well as standard medical practice.

18.2 Safety. For all work performed under this Contract, the Contractor agrees to comply with Department policies and procedures relative to custody of Individuals and security/operation of the institution such as, but not limited to, fingerprinting, photographs for identification purposes, and searches.

19. INDEMNIFICATION

19.1 To the fullest extent permitted by law, Contractor shall indemnify, defend, and hold harmless State, agencies of State and all officials, agents, and employees of State, from and against all claims for injuries or death arising out of or resulting from the performance of the Contract. "Claim" as used in this Contract, means any financial loss, claim, suit, action, damage, or expense, including but not limited to attorney's fees, attributable for bodily injury, sickness, disease, or death, or injury to or destruction of tangible property including loss of use resulting therefrom.

19.2 Contractor's obligation to indemnify, defend and hold harmless includes any claim by Contractors' agents, employees, representatives, or any subcontractor or its employees.

19.3 Contractor expressly agrees to indemnify, defend, and hold harmless the State for any claim arising out of or incident to Contractor's or any subcontractor's performance or failure to perform the Contract. Contractor's obligation to indemnify, defend, and hold harmless the State shall not be eliminated or reduced by any actual or alleged concurrent negligence of State or its agents, agencies, employees and officials.

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

19.5 The provisions of this paragraph shall not apply to any act or omission by the Contractor for which the Department, in the text of this Contract, has agreed to defend and hold the Contractor harmless. The provisions of this section shall survive any termination or the expiration of this Contract.

20. INDEPENDENT CONTRACTOR STATUS

The parties intend that an independent contractor relationship will be created by this Contract. The Contractor will not hold himself or herself out as, nor claim to be, an officer or employee of Washington State in the performance of this Contract. Conduct and control of the work required under this contract is solely with the Contractor.

21. INDUSTRIAL INSURANCE COVERAGE

The Contractor shall comply with the provisions of Title 51 RCW, Industrial Insurance. The Department will not be responsible for payment of industrial insurance premiums or for any other claim or benefit for the Contractor, or any Sub-contractor, or employee of the Contractor, which might arise under these industrial insurance laws during performance of duties and services under this Contract.

22. LICENSING AND ACCREDITATION STANDARDS

The Contractor shall comply with all applicable local, state and federal licensing and accrediting standards, required by law and necessary in the performance of this Contract.

23. LIMITATION OF CONTRACTING AUTHORITY

Only the Secretary, Secretary's designee, or Contracts Administrator shall have the express, implied, or apparent authority to alter, amend, modify, or waive any clause or condition of this contract. Furthermore, any alteration, amendment, modification, or waiver or any clause or condition of this contract is not effective or binding unless made in writing and signed by the Secretary, Secretary's designee, or Contracts Administrator.

24. MAINTENANCE OF RECORDS

24.1 During the term of this Contract and for six (6) years following its termination or expiration, the Contractor shall maintain, and provide DOC or its designee, at no additional cost, with reasonable access to Contractor's records sufficient to:

24.1.1. Document performance of all services required by this Contract; and

24.1.2. Substantiate the Contractor's statement of its organization's structure, tax status, capabilities, performance and principals; and

24.1.3. Demonstrate accounting procedures, practices, and records, which sufficiently and properly document the Contractor's invoices to DOC and all expenditures made by the Contractor to perform as required by this Contract.

24.2 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.

24.3 Should an audit, conducted under the authority of this section, disclose that the Contractor has been paid by the Department in excess of the agreed upon costs (overpayment), or has been reimbursed by the Department for direct or indirect costs which are disallowed as a result of that audit, then, the Contractor shall, upon demand by the Department, repay such overpayment or reimbursement to the Department without requiring further legal action by the Department.

24.4 The provisions of this section shall survive termination or expiration of this Contract.

25. PUBLIC RECORDS ACT

25.1 This Agreement and all records associated with the performance of this Agreement shall be available from the Department for inspection and copying by the public when required by the Public Records Act, Chapter 42.56 RCW (the "Act").

25.2 If records in the custody of the Contractor are needed by the Department to respond to a request under the Act, as determined by the Department, the Contractor agrees to make them promptly available to the Department. Upon request by the Department, the Contractor further agrees to provide a detailed index of records associated with its performance of the contract. This index will allow for more efficient and accurate identification of potentially responsive records.

25.3 If the Contractor considers any portion of any record associated with the Contractor's performance under this Agreement to be protected from disclosure under law, the Contractor shall clearly identify the specific information that it claims to be confidential or proprietary when the records are provided to the Department in response to a public records request. The Department retains sole discretion in the appropriateness and application of withholdings and redactions on all records.

25.4 If the Department receives a request under the Act to inspect or copy information identified by the Contractor as confidential or proprietary and the Department determines that release of the information is required by the Act or otherwise is appropriate, the Department's sole obligation shall be to notify the Contractor (a) of the request and (b) of the date that such information will be released to the requester unless the Contractor obtains a court order to enjoin that disclosure pursuant to RCW 42.56.540. If the Contractor fails to timely obtain a court order enjoining disclosure, the Department will release the requested information on the date specified with whatever withholdings and redactions it deems proper.

25.5 The Department is not obligated to claim any exemption from disclosure under the Act on behalf of the Contractor. The Department shall not be liable to the Contractor for releasing records not clearly identified by the Contractor as confidential or proprietary. The Department shall not be liable to the Contractor for releasing any records in compliance with this section, in compliance with the Act, or in compliance with an order of a court of competent jurisdiction.

26. RECAPTURE OF FUNDS

26.1 In the event that the Contractor fails to perform this contract in accordance with state laws and/or the provisions of this contract, the Department reserves the right to recapture funds in an amount to compensate the Department for the noncompliance in addition to any other remedies available at law or in equity.

26.2 Repayment by the Contractor of funds under this recapture provision shall occur within the time period specified by the Department. In the alternative, the Department may recapture such funds from payments due under this contract.

26.3 Such right of recapture shall exist for a period not to exceed six years following contract termination. In the event that the Department is required to institute legal proceedings to enforce the recapture provision, the Department shall be entitled to its costs thereof, including attorneys' fees.

27. RETIREMENT BENEFIT SUSPENSION – PUBLIC EMPLOYEES RETIREMENT SYSTEM (PERS)

27.1 The Contractor certifies by signing this Contract that that the Contractor is not a Public Employee

Retirement System (PERS) retiree who retired early under the Public Employees Retirement System (PERS) RCW 41.40.630(3); and if it is found that the Contractor did retire early under the PERS, the Contractor's retirement benefits may be suspended for the duration of this Contract.

27.2 Further, if the Contractor was a PERS retiree, the Contractor agrees to notify the Department of Retirement Systems (DRS), regarding the execution of this Contract, failure to do so is considered a material breach and may subject the Contractor to damages. In addition, the Contractor certifies that the Contractor does not have a beneficial interest in this Contract as defined in the Executive Ethics Board's Advisory Opinion 97-07).

28. NONDISCRIMINATION

28.1 During the performance of this contract, the Contractor shall comply with all federal, state, and local nondiscrimination laws, regulations and policies.

28.2 In the event of the Contractor's non-compliance or refusal to comply with any nondiscrimination law, regulation, or policy, this Contract may be rescinded, canceled, or terminated, in whole or in part, and the Contractor may be declared ineligible for further contracts with the Department. The Contractor may be given a reasonable time in which to cure this noncompliance. Any dispute shall be resolved in accordance with the "Disputes" procedure set forth herein.

29. PUBLICITY

The Contractor agrees to submit to the Department all advertising and publicity matters relating to this Contract wherein the Department's name is mentioned or language used from which the connection of the Department's name may, in the Department's judgment, be inferred or implied. The Contractor agrees not to publish or use such advertising and publicity matters without the prior written consent of the Department.

30. REGISTRATION WITH DEPARTMENT OF REVENUE

The 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.

31. RIGHT OF INSPECTION

At no additional cost all records relating to the Contractor's performance under this Contract shall be subject at all reasonable times to inspection, review, and audit by the Department, the Office of the State Auditor, and federal and state officials so authorized by law, in order to monitor and evaluate performance, compliance, and quality assurance under this Contract. The Contractor shall provide access to its facilities for this purpose.

32. RIGHTS AND REMEDIES

The rights and remedies of the Department provided in this Contract shall not be exclusive and are in addition to any other rights and remedies provided by law.

33. SAFEGUARDING OF INCARCERATED INDIVIDUAL INFORMATION

33.1 The Contractor may use Individual information gained by reason of this Contract only to perform work under the terms of this Contract. The Contractor shall not disclose, transfer, or sell any such information to any party, except as provided by law, or with the prior written consent of the Department, Individual, or Individual personal representative.

33.2 The Contractor agrees to abide by all present and future federal and state laws and regulations in maintaining the confidentiality of Department files and records, including Criminal History Record Information (CHRI). In the event CHRI is provided to the Contractor, the Contractor shall also abide by all present and future Department rules and regulations governing the use of CHRI.

33.3 The provisions of this section shall survive any termination or expiration of this Contract.

34. SEVERABILITY

The terms and conditions of this Contract are severable. If any term or condition of this Contract is held invalid by any court, such invalidity shall not affect the validity of the other terms or conditions of this Contract.

35. SITE SECURITY

While on Department premises, Contractor, its agents, employees, or subcontractors shall conform in all respects to site security requirements relative to custody of Individuals and security operations, including but not limited to, background check, fingerprinting, photographs for identification, physical safety, fire, and security policies or regulations.

36. SUBCONTRACTING

36.1 Neither the Contractor nor any Subcontractor shall enter into subcontracts for any of the work contemplated under this Contract without obtaining the prior written approval of the Contracts Administrator. If the Department approves subcontracting, the Contractor shall maintain written procedures related to subcontracting, as well as copies of all subcontracts and records related to subcontracts. For cause, the Department in writing may:

36.1.1. Require the Contractor to amend its subcontracting procedures as they relate to this Contract;

36.1.2. Prohibit the Contractor from subcontracting with a particular person or entity; or

36.1.3. Require the Contractor to rescind or amend a subcontract.

36.2 In no event shall the existence of any subcontract operate to release or reduce the liability of the Contractor to the Department for any breach in the performance of the Contractor's duties. Additionally, the Contractor is responsible for ensuring that all terms, conditions, assurances, and certifications set forth in this Contract are carried forward to any subcontracts.

37. TAXES

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

38. TERMINATION

38.1 BY CONTRACTOR. The Contractor may terminate this Contract by giving the Department written notice of such termination. No such termination shall be effective until sixty (60) days after the Department has received the Contractor's written notice of termination, or until such later date as established by the Contractor in the Contractor's written notice of termination. Contractor shall mail or deliver the Contractor's written notice of termination to the Contracts Administrator. If the Contractor terminates the Contract, the Department shall be liable only for payment in accordance with the terms of this Contract for services rendered prior to the effective date of termination.

38.2 BY DEPARTMENT FOR CAUSE. The Secretary may, by written notice, terminate this Contract in whole or in part, for failure of the Contractor to perform any of the Contract provisions. In such event, the Contractor shall be liable for damages as authorized by law, including, but not limited to, any cost difference between the original Contract and the replacement or cover Contract and all administrative costs directly related to the replacement Contract, i.e., cost of the competitive bidding, mailing, advertising, and staff time. If it is determined for any reason that the Contractor was not in default or that the default was beyond Contractor's or Sub-contractor's control, fault or negligence, then the Termination for Default shall convert to Termination for Convenience.

38.3 In the alternative, the Department upon written notice may allow the Contractor a specific period of time in which to correct the non-compliance. During the corrective-action time period, the Department may suspend further payment to the Contractor in whole or in part, or may restrict the Contractor's right to perform duties under this Contract. Failure by the Contractor to take timely corrective action shall allow the Department to terminate the Contract.

38.4 BY DEPARTMENT FOR CONVENIENCE. The Secretary or designee may terminate this Contract, in whole or in part, when it is in the best interests of the Department. The Department shall give the Contractor written notice of termination at least five days in advance of the effective termination date. When a contract is terminated for convenience, the Department shall only pay, in accordance with the terms of this Contract, for services rendered prior to the effective date of termination.

38.5 BY DEPARTMENT FOR NON-AVAILABILITY OF FUNDS. If the funds the Department relied upon to establish this Contract are withdrawn or reduced, or if new or modified conditions are placed on such funds, the Secretary may terminate this Contract immediately. If this Contract is so terminated, the Department shall be liable only for payment in accordance with the terms of this Contract for services rendered prior to the effective date of termination.

39. TERMINATION PROCEDURES

39.1 Upon termination of this contract the Department shall pay to the Contractor the agreed upon price, if separately stated, for completed work and services accepted by the Department, and the amount agreed upon by the Contractor and the Department for:

39.1.1. Completed work and services for which no separate price is stated;

39.1.2. Partially completed work and services;

39.1.3. Other property or services that are accepted by the Department; and

39.1.4. The protection and preservation of property, unless the termination is for default, in which case the Contracts Administrator shall determine the extent of the liability of the Department. Failure to agree with such determination shall be a dispute within the meaning of the "Disputes" clause of this contract. The Department may withhold from any amounts due the Contractor such sum as the Contracts Administrator determines to be necessary to protect the Department against potential loss or liability.

39.2 The rights and remedies of the Department provided in this "Termination Procedures" provision shall not be exclusive and are in addition to any other rights and remedies provided by law or under this Contract. After receipt of a notice of termination, and except as otherwise directed by the Notice, the Contractor shall:

39.2.1. Stop work under the contract on the date, and to the extent specified, in the notice;

39.2.2. Place no further orders or subcontracts for materials, services, or facilities except as may

be necessary for completion of such portion of the work under the contract that is not terminated;

39.2.3. Assign to the Department, in the manner, at the times, and to the extent directed by the Department, all of the rights, title, and interest of the Contractor under the orders and subcontracts so terminated, in which case the Department has the right, at its discretion, to settle or pay any or all claims arising out of the termination of such orders and subcontracts;

39.2.4. Settle all outstanding liabilities and all claims arising out of such termination of orders and subcontracts, with the approval or ratification of the Department to the extent Department may require, which approval or ratification shall be final for all the purposes of this clause;

39.2.5. Transfer title to the Department and deliver in the manner, at the times, and to the extent directed by the Department any property which, if the contract had been completed, would have been required to be furnished to the Department;

39.2.6. Complete performance of such part of the work as shall not have been terminated by the Department; and

39.2.7. Take such action as may be necessary, or as the Department may direct, for the protection and preservation of the property related to this Contract, which is in the possession of the Contractor and in which the Department has or may acquire an interest.

40. TREATMENT OF PROPERTY

40.1 The Department, in addition to any other rights provided in this Contract, may require the Contractor to deliver to the Department any property specifically produced or acquired for the performance of such part of this Contract as has been terminated. In all such cases, this "Treatment of Property" provision shall apply.

40.2 Title to all property furnished by the Department shall remain in the Department. Title to all property furnished by the Contractor, for the cost of which the Contractor is entitled to be reimbursed as a direct item of cost under this Contract, shall pass to and vest in the Department upon delivery of such property by the Contractor. Title to other property, the cost of which is reimbursable to the Contractor under this Contract, shall pass to and vest in the Department upon i) issuance for use of such property in the performance of this Contract, or ii) commencement of use of such property in the performance of this Contract, or iii) reimbursement of the cost thereof by the Department in whole or in part, whichever first occurs.

40.3 Any property of the Department furnished to the Contractor shall, unless otherwise provided herein or approved by the Department, be used only for the performance of this Contract.

40.4 The Contractor shall be responsible for any loss or damage to Department property that results from the negligence of the Contractor or the failure of the Contractor to maintain and administer that property in accordance with sound management practices.

40.5 If any Department property is lost, destroyed or damaged, the Contractor shall immediately notify the Department and shall take all reasonable steps to protect the property from further damage.

40.6 The Contractor shall surrender all Department property to the Department prior to settlement upon completion, termination, or cancellation of this Contract.

40.7 All equipment purchased by the Contractor for the Contractor's use under the terms of this

Contract, that as defined in this Contract provision, is actually owned by the Department, shall be shipped or delivered to the institution/location designated by the Contract Manager for tagging and entry into the DOC Capital Asset Management System (CAMS) before distribution to the Contractor for use.

41. UTILIZATION OF MINORITY-OWNED AND WOMEN-OWNED BUSINESSES

41.1 During the performance of this Contract, the Contractor shall comply with Chapter 39.19 RCW, as now existing or hereafter amended, any rule adopted under Chapter 39.19 by OMWBE and/or any policy or regulation adopted by the Department to effect agency compliance with Chapter 39.19 RCW.

41.2 If the Contractor fails to comply with any contract requirements relative to the utilization of minority and/or women-owned businesses, the Department may take any or all such actions available to the Department under Chapter 39.19 RCW.

41.3 If the Contractor prevents or interferes with any Subcontractor's compliance with Chapter 39.19 RCW, or submits false or fraudulent information to the Department regarding compliance, the Contractor shall be subject to a fine not to exceed one thousand dollars ($1,000) in addition to any other penalties or sanctions prescribed by law.

42. WAIVER

Waiver of any default or breach shall not be deemed a waiver of any subsequent default or breach. Any waiver shall not be construed to be a modification of the terms of this contract unless stated to be such in writing and signed by authorized representative of the Department.

43. EQUALITY IN COMPENSATION

43.1 The Contractor must ensure that similarly employed individuals in its workforce are compensated as equals, consistent with the following:

Employees are similarly employed if the individuals work for the same employer, the performance of the job requires comparable skill, effort, and responsibility, and the jobs are performed under similar working conditions. Job titles alone are not determinative of whether employees are similarly employed.

Contractor may allow differentials in compensation for its workers based in good faith on any of the following:

i. A seniority system; a merit system; a system that measures earnings by quantity or quality of production; a bona fide job-related factor or factors; or a bona fide regional difference in compensation levels.

ii. A bona fide job-related factor or factors may include, but not be limited to, education, training, or experience, that is: consistent with business necessity; not based on or derived from a gender-based differential; and accounts for the entire differential.

iii. A bona fide regional difference in compensation level must be: consistent with business necessity; not based on or derived from a gender-based differential; and account for the entire differential.

43.2 This Contract may be terminated if the Department or the Department of Enterprise Services

determines that the Contractor is not in compliance with this provision.

44. NONDISCRIMINATION

a. 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.

b. 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).

c. Notwithstanding any provision to the contrary, Agency may suspend Contractor, including any subcontractor, upon notice of a failure to participate and cooperate with any state agency investigation into alleged discrimination prohibited by this Contract, pursuant to RCW 49.60.530(3). Any such suspension will remain in place until Agency receives notification that Contractor, including any subcontractor, is cooperating with the investigating state agency. In the event Contractor, or subcontractor, is determined to have engaged in discrimination identified at RCW 49.60.530(3), Agency may terminate this Contract in whole or in part, and Contractor, subcontractor, or both, may be referred for debarment as provided in RCW 39.26.200. Contractor or subcontractor may be given a reasonable time in which to cure this noncompliance, including implementing conditions consistent with any court-ordered injunctive relief or settlement agreement.

d. Notwithstanding any provision to the contrary, in the event of Contract termination or suspension for engaging in discrimination, Contractor, subcontractor, or both, shall be liable for contract damages as authorized by law including, but not limited to, any cost difference between the original contract and the replacement or cover contract and all administrative costs directly related to the replacement contract, which damages are distinct from any penalties imposed under Chapter 49.60, RCW. Agency shall have the right to deduct from any monies due to Contractor or subcontractor, or that thereafter become due, an amount for damages Contractor or subcontractor will owe Agency for default under this provision.

45. ACCESSIBILITY COMPLIANCE

Contractor hereby warrants that any technology provided under this Agreement currently complies, and will continue to comply, with Washington State Office of Chief Information Officer ("OCIO") Policy 188 (http://ocio.wa.gov/policy/accessibility) and Minimum Accessibility Standard 188.10 (http://ocio.wa.gov/policy/minimum-accessibility-standard). Contractor agrees to promptly respond to and resolve any complaint brought to its attention regarding accessibility of its products or services. Contractor further agrees to indemnify and hold harmless the Washington State Department of Corrections from any claim arising out of Contractor's failure to comply with the aforesaid requirements.

46. WORKER'S RIGHTS

Contractor hereby warrants that it does not require its employees, as a condition of employment, to sign or agree to mandatory individual arbitration clauses or class or collective action waivers.

47. THIRD-PARTY BENEFICIARIES

The Contract entered into between the Parties is for the sole benefit of the Parties hereto and their respective successors and assigns and nothing herein, express or implied, is intended to or shall confer on any other person or entity any legal or equitable right, benefit, or remedy of any nature under or by reason of this Agreement.

Attachment B – DATA SECURITY REQUIREMENTS
& HIPAA COMPLIANCE

HIPAA Compliance

Preamble: This section of the Contract is the Business Associate Agreement as required by HIPAA.

1. **Definitions**.

   a. "Business Associate," as used in this Contract, means the "Contractor" and generally has the same meaning as the term "business associate" at 45 CFR 160.103. Any reference to Business Associate in this Contract includes Business Associate's employees, agents, officers, Subcontractors, third party contractors, volunteers, or directors.

   b. "Business Associate Agreement" means this HIPAA Compliance section of the Contract and includes the Business Associate provisions required by the U.S. Department of Health and Human Services, Office for Civil Rights.

   c. "Breach" means the acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the Protected Health Information, with the exclusions and exceptions listed in 45 CFR 164.402.

   d. "Covered Entity" means DOC, a Covered Entity as defined at 45 CFR 160.103, in its conduct of covered functions by its health care components.

   e. "Designated Record Set" means a group of records maintained by or for a Covered Entity, that is: the medical and billing records about Individuals maintained by or for a covered health care provider; the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or Used in whole or part by or for the Covered Entity to make decisions about Individuals.

   f. "Electronic Protected Health Information (EPHI)" means Protected Health Information that is transmitted by electronic media or maintained in any medium described in the definition of electronic media at 45 CFR 160.103.

   g. "HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, as modified by the American Recovery and Reinvestment Act of 2009 ("ARRA"), Sec. 13400 – 13424, H.R. 1 (2009) (HITECH Act).

   h. "HIPAA Rules" means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Parts 160 and Part 164.

   i. "Individual(s)" means the person(s) who is the subject of PHI and includes a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

   j. "Minimum Necessary" means the least amount of PHI necessary to accomplish the purpose for which the PHI is needed.

k. "Protected Health Information (PHI)" means individually identifiable health information created, received, maintained or transmitted by Business Associate on behalf of a health care component of the Covered Entity that relates to the provision of health care to an Individual; the past, present, or future physical or mental health or condition of an Individual; or the past, present, or future payment for provision of health care to an Individual. 45 CFR 160.103. PHI includes demographic information that identifies the Individual or about which there is reasonable basis to believe can be used to identify the Individual. 45 CFR 160.103. PHI is information transmitted or held in any form or medium and includes EPHI. 45 CFR 160.103. PHI does not include education records covered by the Family Educational Rights and Privacy Act, as amended, 20 USCA 1232g(a)(4)(B)(iv) or employment records held by a Covered Entity in its role as employer.

l. "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.

m. "Subcontractor" as used in this HIPAA Compliance section of the Contract (in addition to its definition in the General Terms and Conditions) means a Business Associate that creates, receives, maintains, or transmits Protected Health Information on behalf of another Business Associate.

n. "Use" includes the sharing, employment, application, utilization, examination, or analysis, of PHI within an entity that maintains such information.

2. **Compliance**. Business Associate shall perform all Contract duties, activities and tasks in compliance with HIPAA, the HIPAA Rules, and all attendant regulations as promulgated by the U.S. Department of Health and Human Services, Office of Civil Rights.

3. **Use and Disclosure of PHI**. Business Associate is limited to the following permitted and required uses or disclosures of PHI:
   a. Duty to Protect PHI. Business Associate shall protect PHI from, and shall use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 (Security Standards for the Protection of Electronic Protected Health Information) with respect to EPHI, to prevent the unauthorized Use or disclosure of PHI other than as provided for in this Contract or as required by law, for as long as the PHI is within its possession and control, even after the termination or expiration of this Contract.

   b. Minimum Necessary Standard. Business Associate shall apply the HIPAA Minimum Necessary standard to any Use or disclosure of PHI necessary to achieve the purposes of this Contract. See 45 CFR 164.514 (d)(2) through (d)(5).

   c. Disclosure as Part of the Provision of Services. Business Associate shall only Use or disclose PHI as necessary to perform the services specified in this Contract or as required by law, and shall not Use or disclose such PHI in any manner that would violate Subpart E of 45 CFR Part 164 (Privacy of Individually Identifiable Health Information) if done by Covered Entity, except for the specific uses and disclosures set forth below.

d. Use for Proper Management and Administration. Business Associate may Use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

e. Disclosure for Proper Management and Administration. Business Associate may disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of the Business Associate, provided the disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been Breached.

f. Impermissible Use or Disclosure of PHI. Business Associate shall report to DOC in writing all Uses or disclosures of PHI not provided for by this Contract within one (1) business day of becoming aware of the unauthorized Use or disclosure of PHI, including Breaches of unsecured PHI as required at 45 CFR 164.410 (Notification by a Business Associate), as well as any Security Incident of which it becomes aware. Upon request by DOC, Business Associate shall mitigate, to the extent practicable, any harmful effect resulting from the impermissible Use or disclosure.

g. Failure to Cure. If DOC learns of a pattern or practice of the Business Associate that constitutes a violation of the Business Associate's obligations under the terms of this Contract and reasonable steps by DOC do not end the violation, DOC shall terminate this Contract, if feasible. In addition, If Business Associate learns of a pattern or practice of its Subcontractors that constitutes a violation of the Business Associate's obligations under the terms of their contract and reasonable steps by the Business Associate do not end the violation, Business Associate shall terminate the Subcontract, if feasible.

h. Termination for Cause. Business Associate authorizes immediate termination of this Contract by DOC, if DOC determines that Business Associate has violated a material term of this Business Associate Agreement. DOC may, at its sole option, offer Business Associate an opportunity to cure a violation of this Business Associate Agreement before exercising a termination for cause.

i. Consent to Audit. Business Associate shall give reasonable access to PHI, its internal practices, records, books, documents, electronic data and/or all other business information received from, or created or received by Business Associate on behalf of DOC, to the Secretary of DHHS and/or to DOC for use in determining compliance with HIPAA privacy requirements.

j. Obligations of Business Associate Upon Expiration or Termination. Upon expiration or termination of this Contract for any reason, with respect to PHI received from DOC, or created, maintained, or received by Business Associate, or any Subcontractors, on behalf of DOC, Business Associate shall:

k. Retain only that PHI which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;

l. Return to DOC or destroy the remaining PHI that the Business Associate or any Subcontractors still maintain in any form;

m. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 (Security Standards for the Protection of Electronic Protected Health Information) with respect to Electronic Protected Health Information to prevent Use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate or any Subcontractors retain the PHI;

n. Not Use or disclose the PHI retained by Business Associate or any Subcontractors other than for the purposes for which such PHI was retained and subject to the same conditions set out in the "Use and Disclosure of PHI" section of this Contract which applied prior to termination; and

o. Return to DOC or destroy the PHI retained by Business Associate, or any Subcontractors, when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

p. Survival. The obligations of the Business Associate under this section shall survive the termination or expiration of this Contract.

4. **Individual Rights**. Accounting of Disclosures.

a. Business Associate shall document all disclosures, except those disclosures that are exempt under 45 CFR 164.528, of PHI and information related to such disclosures.

b. Within ten (10) business days of a request from DOC, Business Associate shall make available to DOC the information in Business Associate's possession that is necessary for DOC to respond in a timely manner to a request for an accounting of disclosures of PHI by the Business Associate. See 45 CFR 164.504(e)(2)(ii)(G) and 164.528(b)(1).

c. At the request of DOC or in response to a request made directly to the Business Associate by an Individual, Business Associate shall respond, in a timely manner and in accordance with HIPAA and the HIPAA Rules, to requests by Individuals for an accounting of disclosures of PHI.

d. Business Associate record keeping procedures shall be sufficient to respond to a request for an accounting under this section for the six (6) years prior to the date on which the accounting was requested.

5. Access.

a. Business Associate shall make available PHI that it holds that is part of a Designated Record Set when requested by DOC or the Individual as necessary to satisfy DOC's obligations under 45 CFR 164.524 (Access of Individuals to Protected Health Information).

b. When the request is made by the Individual to the Business Associate or if DOC asks the Business Associate to respond to a request, the Business Associate shall comply with requirements in 45 CFR 164.524 (Access of Individuals to Protected Health Information) on form, time and manner of access. When the request is made by DOC, the Business Associate shall provide the records to DOC within ten (10) business days.

6. **Amendment**.

a. If DOC amends, in whole or in part, a record or PHI contained in an Individual's Designated Record Set and DOC has previously provided the PHI or record that is the subject of the amendment to Business Associate, then DOC will inform Business Associate of the amendment pursuant to 45 CFR 164.526(c)(3) (Amendment of Protected Health Information).

b. Business Associate shall make any amendments to PHI in a Designated Record Set as directed by DOC or as necessary to satisfy DOC's obligations under 45 CFR 164.526 (Amendment of Protected Health Information).

7. **Subcontracts and other Third Party Agreements**. In accordance with 45 CFR 164.502(e)(1)(ii), 164.504(e)(1)(i), and 164.308(b)(2), Business Associate shall ensure that any agents, Subcontractors, independent contractors or other third parties that create, receive, maintain, or transmit PHI on Business Associate's behalf, enter into a written contract that contains the same terms, restrictions, requirements, and conditions as the HIPAA compliance provisions in this Contract with respect to such PHI. The same provisions must also be included in any contracts by a Business Associate's Subcontractor with its own business associates as required by 45 CFR 164.314(a)(2)(b) and 164.504(e)(5).

8. **Obligations**. To the extent the Business Associate is to carry out one or more of DOC's obligation(s) under Subpart E of 45 CFR Part 164 (Privacy of Individually Identifiable Health Information), Business Associate shall comply with all requirements that would apply to DOC in the performance of such obligation(s).

9. **Liability**. Within ten (10) business days, Business Associate must notify DOC of any complaint, enforcement or compliance action initiated by the Office for Civil Rights based on an allegation of violation of the HIPAA Rules and must inform DOC of the outcome of that action. Business Associate bears all responsibility for any penalties, fines or sanctions imposed against the Business Associate for violations of the HIPAA Rules and for any imposed against its Subcontractors or agents for which it is found liable.

10. **Breach Notification**.

a. In the event of a Breach of unsecured PHI or disclosure that compromises the privacy or security of PHI obtained from DOC or involving DOC clients, Business Associate will take all measures required by state or federal law.

b. Business Associate will notify DOC within one (1) business day by telephone and in writing of any acquisition, access, Use or disclosure of PHI not allowed by the provisions of this Contract or not authorized by HIPAA Rules or required by law of which it becomes aware which potentially compromises the security or privacy of the Protected Health Information as defined in 45 CFR 164.402 (Definitions).

c. Business Associate will notify the DOC Contact shown on the cover page of this Contract within one (1) business day by telephone or e-mail of any potential Breach of security or privacy of PHI by the Business Associate or its Subcontractors or agents. Business Associate will follow telephone or e-mail notification with a faxed or other written explanation of the Breach, to include the following: date and time of the Breach, date Breach was discovered, location and nature of the PHI, type of Breach, origination and destination of PHI, Business Associate unit and personnel associated with the Breach, detailed description of the Breach, anticipated mitigation steps, and the name, address, telephone number, fax number, and e-mail of the individual who is responsible as the primary point of contact. Business Associate will address communications to the DOC Contact. Business Associate will coordinate and cooperate with DOC to provide a copy of its investigation and other information requested by DOC, including advance copies of any notifications required for DOC review before disseminating and verification of the dates notifications were sent.

d. If DOC determines that Business Associate or its Subcontractor(s) or agent(s) is responsible for a Breach of unsecured PHI:

(1) requiring notification of Individuals under 45 CFR § 164.404 (Notification to Individuals), Business Associate bears the responsibility and costs for notifying the affected Individuals and receiving and responding to those Individuals' questions or requests for additional information;

(2) requiring notification of the media under 45 CFR § 164.406 (Notification to the media), Business Associate bears the responsibility and costs for notifying the media and receiving and responding to media questions or requests for additional information;

(3) requiring notification of the U.S. Department of Health and Human Services Secretary under 45 CFR § 164.408 (Notification to the Secretary), Business Associate bears the responsibility and costs for notifying the Secretary and receiving and responding to the Secretary's questions or requests for additional information; and;

(4) DOC will take appropriate remedial measures up to termination of this Contract.

11. **Miscellaneous Provisions**.

a. Regulatory References. A reference in this Contract to a section in the HIPAA Rules means the section as in effect or amended.

b. Interpretation. Any ambiguity in this Contract shall be interpreted to permit compliance with the HIPAA Rules.

Category 3
Data Security Requirements

1. Definitions. The words and phrases listed below, as used in this Attachment, 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 DOC Confidential Information, and who has or have been authorized to do so.

c. "Business Associate Agreement" means an agreement between DOC 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 3 Data" is Confidential information is information that is specifically protected from either release or disclosure by law. This includes, but is not limited to:

1. Personal information as defined in RCW 42.56.590 and RCW 19.255.10.

2. Information about public employees as defined in RCW 42.56.250.

3. Lists of individuals for commercial purposes as defined in RCW 42.56.070

4. Information about the infrastructure and security of computer and telecommunication networks as defined in RCW 42.56.420.

e. "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.

f. “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.

g. “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.

h. “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.

i. “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.

j. “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.

k. “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.

l. “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.

m. “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.

n. “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.

o. "Trusted Network" means a network operated and maintained by the Contractor, which includes security controls sufficient to protect DOC 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.

p. "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.

q. "Biometric identifier" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's retina or iris scan, fingerprint, voiceprint, DNA, or scan of hand or face geometry, except when such information is derived from:

(i) Writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color;

(ii) Donated organ tissues or parts, or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency;

(iii) Information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal health insurance portability and accountability act of 1996; or

(iv) X-ray, roentgen process, computed tomography, magnetic resonance imaging (MRI), positron emission tomography (PET) scan, mammography, or other image or film of the human anatomy used to diagnose, develop a prognosis for, or treat an illness or other medical condition or to further validate scientific testing or screening.

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, WA DOC Policy 280.310 – Information Technology Security; WA DOC Policy 280.515 – Data Classification and Sharing; the terms and conditions set forth in this Agreement; and all applicable state and federal laws in its treatment of WA DOC Data

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. Any data center security controls must meet or exceed those expected by the Federal

Information Security Management Act (FISMA) for low to moderate impact systems as described in FIPS 199 and 200, and in the most current release of National Institute of Standards and Technology (NIST) Special Publications SP800- 53, including all other referenced NIST publications.

c. Contractor warrants that all data collected, processed, routed, and/or stored by or through the service, or third-party service providers, remains at all times within the United States.

d. 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.

e. 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 DOC 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 networks (using key lengths of 128 bits or greater) Algorithm modules validated by the National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) are required. 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 20 minutes of inactivity.

(6) Ensuring use of Multi-factor Authentication to connect from the external end point to the internal end point. Authentication mechanisms must meet or exceed those described in the most recent version of NIST SP 800-63 for information requiring assurance level 3 or higher. One of the authentication factors should be provided by a device separate from the computer gaining access.

(7) Ensuring all system and service accounts use Enterprise Active Directory or a similar centralized authentication and authorization mechanism. If authentication methods such as SQL authentication are required by the system, Contractor uses credentials secured during transmission through encrypted sessions such as TLS1.2 (or greater) or IPSec, and in storage using a secure hash method validated by the National Institute of Standards and Technology (NIST). Within 72 hours of a request from DOC, Contractor must provide documentation showing how the credentials are secured during all transmissions using encrypted sessions such as TLS or IPSec, and in storage using a secure hash method validated by the National Institute of Standards and Technology (NIST).

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.

l. Ensure the system/service supports single sign-on for state government employees, and external users by integrating the system's authentication mechanisms with the Washington State Enterprise Active Directory and Secure Authentication Gateways (post listeners are typically used for processing the gateway host headers).

m. Utilize application authentication controls that are consistent with those described in the most recent version of NIST SP 800-63 for information requiring assurance level 2 or higher.

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

(1) DOC 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 DOC.

(f) The Data will not be downloaded to non-authorized systems, meaning systems that are not on either the DOC 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 DOC 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 DOC Data or through which that Data passes:

a. Systems containing DOC 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 DOC 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. These anti-malware practices must meet or exceed those described in NIST SP800-40.

e. The architecture must provide continuous monitoring of both internal and external activity for anomalies and identify, report, and defend against security intrusions before data is compromised.

f. Contractor shall conduct penetration tests at least once every 24 months, system vulnerability assessments at least monthly, and application vulnerability assessments prior to the production release of any changes to source code.

g. Contractor has implemented application/system development practices consistent with the current version of NIST SP800-64 for low to moderate impact systems, and warrants the software does not contain any of the Open Web Application Security project (OWASP) top 10 vulnerabilities - https://www.owasp.org/index.php/Main_Page

h. Contractor has a practice of systematic collection, monitoring, alerting, maintenance, retention, and disposal of security event logs and application audit trails. Logs and audit trails are written to an area inaccessible to system users and are protected from editing. At a minimum the logs and audit trails will provide historical details on all transactions within the system that are necessary to reconstruct activities. Including recording; type of event, date, time, account identification and machine identifiers for each logged transaction. Audit and log files can be analyzed by type in order to find emerging issues or trends. Contractor has settings triggering an immediate notification to appropriate system administrators for severe incidents. Logs are secured against unauthorized changes. At a minimum, logs must be retained for a period of 6 months.

7. Data Segregation.

a. DOC Data must be segregated or otherwise distinguishable from non-DOC data. This is to ensure that when no longer needed by the Contractor, all DOC Data can be identified for return or destruction. It also aids in determining whether DOC 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) DOC Data will be kept on media (e.g. hard disk, optical disc, tape, etc.) which will contain no non-DOC Data. And/or,

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

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

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

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

b. When it is not feasible or practical to segregate DOC Data from non-DOC data, then both the DOC Data and the non-DOC 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 DOC 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**. Contractor shall implement incident response practices consistent with NIST SP 800-61. The actual compromise of DOC Data must be reported to the DOC Contact designated in the Contract within three (3) business days of discovery. If no DOC Contact is designated in the Contract, then the notification must be reported to the DOC Contracts and Legal Affairs office at docclacontracts@doc1.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 DOC.

10. **Data shared with Subcontractors**. If DOC 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 DOC Contact specified for this contract for review and approval.

11. **System Audit Requirements**. Contractor has completed a recent independent security audit by a SOC 2 Type 2 accredited firm of their development and operational practices, or that an independent security audit by an accredited firm will be completed within 6 months after contract execution. This audit must include vulnerability assessments, and penetration tests, and confirm compliance with the security requirements herein. The audit should include any specific data center facility where the service is deployed, and all failover facilities unless those facilities provide their own SOC 2 Type 2 audit.

12. **Disaster Recovery**. Contractor shall document, test and maintain a disaster recovery plan including an alternate facility to assure the system/service is recovered within 24 hours of a force majeure event. The recovery plan must protect against more than 24 hours of DOC data being lost.

13. **Records Maintenance**. The parties to this Agreement shall each maintain books, records, documents, and other evidence which sufficiently and properly reflect all direct and indirect costs expended by either party in the performance of the services described herein, if any. These records shall be subject to inspection, review, or audit by personnel of both parties, other personnel duly authorized by either party, the Office of the State Auditor, and federal officials so authorized by law. All books, records, documents, and other material relevant to this Agreement will be retained for six (6) years after expiration and the Office of the State Auditor, federal auditors, and any persons duly authorized by the parties shall have full access and the right to examine any of these materials during this period.

14. **Rights in Data**. Unless otherwise provided in this Agreement, this Agreement will not be construed to effect any transfer of right or license to the embodiments of the Washington DOC's Data, except to the limited extent necessary to carry out the responsibilities specified herein. Commercialization of DOC Category 3 or Category 4 data, or sharing of DOC data with third parties without the written permission of DOC is strictly prohibited under these terms.

15. **Insurance Requirements.** If this agreement involves the Contractor collecting, storing, creating, altering, processing, transmitting, routing, or handling any DOC Category 3 or Category 4 data, then Contractor shall obtain and maintain for the duration of the Contract, at Contractor's expense, the following insurance coverages which the parties agree are unaffected by any limitation of liability language within this Agreement.

a. Technology Professional Liability (errors and omissions)

The Contractor shall maintain Technology Professional Liability (errors and omissions) insurance, to include coverage of claims involving infringement of intellectual property. This shall include but is not limited to infringement of copyright, trademark, trade dress, invasion of privacy violations, information theft, damage to or destruction of electronic information, release of private information, alteration of electronic information, extortion, network security, regulatory defense (including fines and penalties), and notification costs. The coverage limits must be at least $1,000,000 per covered claim without sublimit, and $2,000,000 annual aggregate.

b. Crime and Employee Dishonesty

The Contractor shall maintain Employee Dishonesty and (when applicable) Inside/Outside Money and Securities coverages for property owned by the State of Washington in the care, custody, and control of Contractor, to include electronic theft and fraud protection. The coverage limits must be at least $1,000,000 per covered claim without sublimit, $2,000,000 annual aggregate.

c. Cyber Risk Liability Insurance

The Contractor shall maintain coverage for Cyber Risk Liability, including information theft, computer and data loss replacement or restoration, release of private information, alteration of electronic information, notification costs, credit monitoring, forensic investigation, cyber extortion, crises management, public relations expenses, regulatory defense (including fines and penalties), network security, and liability to third parties from failure(s) of contractor to handle, manage, store, and control personally identifiable information belonging to others. The policy must include full prior acts coverage. The coverage limits must be at least $1,000,000 per covered claim without sublimit, $2,000,000 annual aggregate.