Washington State
Department of Corrections

Contract No. K12843
Amendment No. 4

This Amendment is made by the Washington State Department of Corrections, hereinafter referred to as "DOC" or "Department," and the City of Sunnyside, hereinafter referred to as "City" or "Contractor," for the purpose of amending the above-referenced Contract, heretofore entered into between Department and Contractor.

WHEREAS the purpose of this Amendment is to extend the term, update the per diem billing rate, add data sharing terms and conditions, and add language regarding the last day bed payment by updating the definition of "Offender day," modifying related sections, and replacing Attachment C. A term is also replaced.

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

Replacement of Terms. All occurrences of the term "Offender" and "offender" in the Agreement shall be replaced with the term "Incarcerated Individual." All such replacements shall be applicable for the singular, plural, and possessive forms of the respective terms thereof.

ARTICLE I, SECTION 1.13 is hereby amended as follows:

Section 1.13 **((~~Offender day~~)) Incarcerated Individual day** – means any day a Department ((~~offender~~)) Incarcerated Individual is in the custody of the Contractor including the first and last day the ((~~offender~~)) Incarcerated Individual is sanctioned or held by the Department to a term of confinement to be served in the Facility.

Section 1.13.1 An ((~~offender day~~)) Incarcerated Individual day ends at midnight ((~~of the day immediately preceding the day~~)) of the ((~~offender's~~)) Incarcerated Individual's release from the Department's sanction, transferred to a Department institution, transferred to another Facility, released to the custody of the Department, or released to the community.

Section 1.13.2 An ((~~offender~~)) Incarcerated Individual day shall not include any day that is by state law the financial responsibility of the Contractor or any other jurisdiction.

ARTICLE II, SECTION 2.1 is hereby amended as follows:

Section 2.1 **Term.** This Agreement supersedes all previous oral and written contracts and agreements between the parties relating to the confinement, care, and treatment of Department ((~~offenders~~)) Incarcerated Individuals. This Contract commences on ((~~October 01, 2020~~)) January 01, 2021, and continues through ((~~June 30, 2024~~)) June 30, 2026, unless terminated by either party pursuant to this Contract.

ARTICLE II, SECTION 2.4 is hereby amended, in part, as follows:

Section 2.4 Per Diem Billing. [....] From January 01, 2024, through June 30, 2024, the per diem rate is $57.16 per Department ((~~offender~~)) Incarcerated Individual. The per diem rate for July 1, 2024, to June 30, 2025, is $60.02, and the per diem rate for July 1, 2025, to June 30, 2026, is $63.02. The Department will pay $70.00 per Department ((~~offender~~)) Incarcerated Individual for transport to Yakima County Jail. [....]

> **Section 2.4.2** The Department's financial responsibilities under this Contract terminate ((~~when the Department takes custody of the Department offender, when the Department's sanction has been served, or when the Department's hold or detainer is no longer valid, whichever is earlier.~~)) at midnight on the day of the earliest occurring of the following:
>
> - Department takes custody of the Department Incarcerated Individual;
> - Department's sanction has been served; or
> - Department's hold or detainer is no longer valid.

ATTACHMENT C, OFFENDER HOUSING INVOICE/ MEDICAL BILLING REIMBURSEMENT FORM is hereby replaced in its entirety by **ATTACHMENT C-1, MEDICAL BILLING REIMBURSEMENT FORM/ INCARCERATED INDIVIDUAL HOUSING INVOICE,** which is attached hereto and incorporated by reference herein.

ATTACHMENT D, DATA SHARING AND ACCESS TO INFORMATION TECHNOLOGY RESOURCES TERMS AND CONDITIONS, which is attached hereto and incorporated herein, is added and incorporated into the Contract as though fully set forth therein.

Additions to this text are shown by underline and deletions by ((~~strikeout~~)). All other terms and conditions remain in full force and effect. The effective date of this amendment is **July 01, 2024.**

[Remainder of this page intentionally left blank. Signature page follows.]

THIS CONTRACT AMENDMENT, consisting of three (3) pages and two (2) attachments, is executed by the persons signing below who warrant that they have the authority to execute the contract.

CITY OF SUNNYSIDE

11/21/24

City Manager Date

DEPARTMENT OF CORRECTIONS

Daryl Huntsinger Date
Contracts Administrator

ATTEST (if needed by County):

11/18/2024

City Clerk Date

CITY CONTRACT NO: A-2024-133
RESOLUTION NO: 2014-55
COUNCIL MTG: X

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

ATTACHMENT C-1

MEDICAL BILLING REIMBURSEMENT FORM/ INCARCERATED INDIVIDUAL HOUSING INVOICE

(County/City/Tribal) Jail
(Street Address)
(Phone Number)

(Month) 2015
Total Amount ($00.00)

Bill to:
Washington State Department of Correction
P.O. Box 41149
Olympia, WA 98504 (360) 725-8620
DOCViolatorbedbilling@DOC1.WA.GOV

Daily Bed Day Rate: $65.00

Name	DOC #	DOB	DOC start date Sanction/Confinement	DOC End/Transfer date for Sanction/Confinement	Total # of billed DOC Days	Total amount billed to DOC
Doe, Jane	123456	1/15/89	7/19/15	7/21/15	3	$195.00
Smith, Johnny	121212	2/26/62	7/8/15	7/20/15	13	$845.00
County Border Exchange Days:						
Jahnsen, Doe	5555555	10/31/92	8/1/15	8/1/15	1	$65.00
TOTAL					17	$1,105.00

Last Name	First Name	DOC#	Date of Birth	Date of Service	Medical Facility or RX name, & strength	RX quantity or # of days	RX # or reason for treatment	Name of jail staff contacting DOC medical staff	Date and time of contact with medical staff	Name of DOC medical staff contacted	Copy of approved non-formulary request attached, if available? Y, N or N/A	Copy of off-site medical provider claim form and/or Contractors' original pharmacy bill attached as required? Y/N	Amount of copay paid by Incarcerated Individual if any	Amount paid by contractor	Amount billed to DOC
Doe	Jane	123456	1/15/89	7/20/15	Gabapentin 30 MG Tab	3 pills	1234561	Elmer Phud	7/20/15; 12:34 pm	Tammy Williams	Y	Y	$1.00	$12.50	$11.50
Smith	Johnny	121212	2/26/62	7/10/15	St Joseph's Hospital	7 days	Chest pain	Erin Rogers	7/10/15; 2:40 am	Lisa Russell-Tutty	N/A	Y	$ -	$2,500.00	$2,500.00
Jahnsen	Doe	555555	10/31/92	8/1/15	Walla-Walla General Hospital	5 weeks	Foreign object removal	Billie Goat	8/1/15: 4:10 pm	Sarah Nichols	N/A	Pending	$4.00	$5,000.00	$4,996.00

ATTACHMENT D

DATA SHARING AND ACCESS TO INFORMATION TECHNOLOGY RESOURCES TERMS AND CONDITIONS

1. GENERAL

1.1 The purpose of the Data Sharing and Access to Information Technology Resources Terms and Conditions is to set forth the terms and conditions under which the Department of Corrections ("WADOC") will allow the restricted use of its confidential information to City of Sunnyside ("Requestor"), and under which Requestor may receive and use the confidential information. This Agreement further sets forth the terms and conditions under which WADOC will allow the restricted use of and access to its information technology (IT) resources ("IT Resources") and under which Requestor may access and use those IT Resources. This Agreement ensures that confidential information and access to IT resources are provided, protected, and used only for purposes authorized by this Agreement and in accordance with state and federal law.

1.2 WADOC may provide Requestor with confidential information necessary for Requestor to perform the Agreement, including Protected Health Information of individuals under the jurisdiction of the Department.

1.3 The data to be shared under this Agreement may include Category 3 — Confidential Information and Category 4 — Confidential Information Requiring Special Handling, based upon classification categories developed by the Washington State Office of the Chief Information Officer (hereinafter referred to as "OCIO"). Data will be on an individual-level and non-aggregated, with personal identifiers. All data and information provided to Requestor by Department pursuant to this Agreement is hereinafter referred to as "WADOC Data."

2. USE OF DATA AND IT RESOURCES

2.1 Requestor and its employees, agents, volunteers, contractors, and subcontractors (collectively referred to herein as "Requestor") with access to WADOC Data and/or IT Resources shall access and use such data and/or resources only for the purposes set forth in this Agreement. This Agreement does not constitute a release of WADOC Data and/or IT Resources for Requestor's discretionary use. WADOC Data and IT Resources may be accessed only to carry out the responsibilities specified herein. Any ad hoc analyses or other use of WADOC Data or IT Resources not specified in this Agreement is not permitted without the prior written agreement of WADOC.

2.2 Requestor shall comply with the policies, standards, and guidelines of the OCIO; WADOC Policy 280.310 – Information Technology Security; WADOC 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 WADOC Data and IT Resources.

2.3 Neither the state of Washington nor WADOC guarantee or warrant the accuracy, timeliness, or completeness of WADOC Data. Requestor understands and assumes all risks and liabilities of use and misuse of WADOC Data or IT Resources by Requestor.

2.4 Requestor shall not use, transfer, sell, or otherwise disclose WADOC Data gained by reason of this Agreement for any purpose that is not directly connected with the purpose, justification, and permitted uses of this Agreement, except as provided by law or with the prior written consent of WADOC and the individual or personal representative of the individual who is the subject of the WADOC Data, if any.

2.5 (Omitted.)

2.5.1 (Omitted.)

2.5.2 (Omitted.)

2.5.3 (Omitted.)

2.6 Requestor is not authorized to update or change any WADOC Data, and any updates or changes to WADOC Data shall be cause for immediate termination of this Agreement.

2.7 PUBLICATION OF WADOC DATA.

2.7.1 Any and all reports utilizing or derived from WADOC Data shall be subject to review by WADOC prior to publication or presentation. Requestor shall provide all draft materials to WADOC for review of usability, data sensitivity, data accuracy, completeness, and consistency with WADOC standards at least twenty (20) working days prior to the presentation or publication of any report utilizing or derived from WADOC Data.

2.7.2 Requestor shall include the following statement with any publication utilizing or derived from WADOC Data:

> "This material utilizes confidential information from the Washington State Department of Corrections (WADOC). Any views expressed here are those of the author(s) and do not necessarily represent those of the WADOC or other data contributors. Any errors are attributable to the author(s)."

2.8 Any data that is derived from WADOC Data or which could not have been produced but for the use of WADOC Data shall be considered WADOC Data and is subject to the terms and conditions set forth in this Agreement.

2.9 The requirements in this section shall survive the termination or expiration of this Agreement or any subsequent agreement intended to supersede this Agreement.

3. DATA SECURITY

3.1 PROTECTION OF DATA. All electronic data provided by WADOC shall be stored on an encrypted hard drive in a secure environment with access limited to the fewest number of staff needed to complete the purpose of this Agreement.

3.1.1 Workstation hard disk drives. Data stored on local workstation hard disks shall be encrypted with a FIPS approved cryptographic algorithm. Access will be restricted to authorized users by requiring logon to the local workstation using a unique user ID and complex password or other authentication mechanisms that provide equal or greater security, such as biometrics or smart cards.

3.1.2 Network server disks. Data stored on hard disks mounted on network servers and made available through shared folders shall be encrypted with a FIPS approved cryptographic algorithm. 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 complex 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. Backup copies must be encrypted if recorded to removable media.

3.1.3 Optical discs (e.g., CDs, DVDs, Blu-Rays) in local workstation optical disc drives. Data provided by WADOC on optical discs that will be used in local workstation optical disc drives and will not be transported out of a secure area shall be encrypted with a FIPS approved cryptographic algorithm. When not in use, such discs must be locked in a drawer, cabinet or other container to which only authorized users have the key combination, or mechanism required to access the contents of the container. Workstations which access WADOC Data on optical discs must be located in an area accessible only to authorized individuals, with access controlled though use of key, card key, combination lock, or comparable mechanism.

3.1.4 Optical discs (e.g., CDs, DVDs, Blu-Rays) in drives or other devices attached to a network. Data provided by WADOC on optical discs that will be used in drives or other devices attached to a network shall be encrypted with a FIPS approved cryptographic algorithm. 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 complex password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. The optical discs must be located in an area accessible only to authorized individuals, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

3.1.5 Paper documents. Any paper records must be protected by storing the records in a secure area accessible only to authorized individuals. When not in use, such records must be stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.

3.1.6 Portable Devices. Within this Agreement, portable devices include, but are not limited to handhelds/PDAs, Ultramobile PCs, flash memory devices (e.g., USB flash drives, personal media players), portable hard disks, and laptop/notebook computers. Portable media includes, but is not limited to optical media (e.g., CD's, DVD's, Blu-Rays), magnetic media (e.g., floppy disks, Zip or Jaz disks or drives), and flash media (e.g., Compact Flash, SD Card, MMC).

- Requestor shall not store WADOC Data on portable devices or portable media unless specifically authorized within this Agreement. If so authorized, the Requestor shall:

- Encrypt the data with a FIPS approved cryptographic algorithm.

- Control access to devices with a unique user ID and password or stronger authentication method such as a physical token or biometrics.

- 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 twenty (20) minutes.

- Physically protect the portable device(s) and/or media by keeping them in locked storage when unused; using check-in/check-out procedures when device or other media is being shared; taking frequent inventories of media, and access to media by users.

- When being transported outside of a secure area, portable devices and media with confidential WADOC Data must be under the physical control of Requestor's staff with authorization to access the data.

3.1.7 Backup Data Storage

3.1.7.1 WADOC Data may be stored on Portable Devices that meet the requirements for such storage as part of Requestor'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 normal backup operations. If backup media is retired while WADOC Data still exists upon it, such media will be destroyed at that time in accordance with the disposition requirements of this Agreement.

3.1.7.2 Data may be stored on non-portable media (e.g., Storage Area Network drives, virtual media, etc.) that meet the requirements for such storage as part of a Requestor's existing, documented backup process for business continuity or disaster recovery purposes. If so, such media will be protected as otherwise described in this Agreement. If this media is retired while WADOC Data still exists upon it, the WADOC Data will be destroyed at that time in accordance with the disposition requirements of this Agreement.

3.1.8 Cloud Storage. WADOC Data requires protections equal to or greater than those specified in this agreement. Cloud storage of WADOC Data is problematic as neither DOC nor the Requestor has control of the environment in which the WADOC Data is stored. For this reason:

3.1.8.1 WADOC Data will not be stored in any consumer grade Cloud solution, unless all of the following conditions are met:

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

(2) WADOC Data will be Encrypted while within the Requestor's network.

(3) WADOC Data will remain Encrypted during transmission to the Cloud.

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

(5) Requestor will possess a decryption key for the WADOC Data and the decryption key will be possessed only by Requestor and/or DOC.

(6) WADOC Data will not be downloaded to non-authorized systems, meaning systems that are not on either the DOC network or Requestor's network.

(7) WADOC Data will not be decrypted until downloaded onto a computer within the control of an Authorized User and within either the DOC's network or Requestor's network.

3.1.8.2 WADOC Data will not be stored on an Enterprise Cloud storage solution unless either:

(1) The Cloud storage provider is treated as any other subcontractor and agrees in writing to all the requirements within this Attachment; or

(2) The cloud storage solution used is FedRAMP certified.

3.1.8.3 If WADOC 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 storing WADOC Data in their Cloud solution.

3.1.8.4 Definitions. The words and phrases used in this provision shall have the following definitions:

(1) "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.

(2) "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.

(3) "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.

(4) "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.

3.2 SYSTEM PROTECTION. To prevent the compromise of systems that contain WADOC Data or through which WADOC passes:

3.2.1 Systems containing WADOC Data must have all security patches or hotfixes applied within three (3) months after such patches or hotfixes are made available.

3.2.2 Requestor must have a process to ensure that the requisite patches and hotfixes have been identified and applied within the required timeframe.

3.2.3 Systems containing WADOC Data shall have anti-malware application installed, if such an application is available.

3.2.4 Anti-malware software shall be kept up to date. The product, anti-virus engine, and any malware database used will be no more than one (1) update behind the most current version.

3.2.5 Requestor's patch management process must meet or exceed the then-current standards promulgated by the National Institute of Standards and Technology (NIST), which may be found at the time of drafting in NIST Special Publication 800-40.

3.2.6 The system 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.

3.2.7 Requestor shall conduct penetration tests at least once every twenty-four (24) months, system vulnerability assessments at least monthly, and application vulnerability assessments prior to the production release of any changes to source code.

3.2.8 Requester's application/system development practices must be consistent with those promulgated by NIST for low to moderate impact systems, which may be found in NIST SP 800.64 at the time of drafting.

3.2.9 Requestor warrants that its application/system does not contain any of the Open Web Application Security Project's top ten (10) vulnerabilities.

3.2.10 Requestor 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 must provide historical details on all transactions within the system that are necessary to reconstruct activities, including, but not limited to, recording the 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. Requestor's system must trigger immediate notification to appropriate system administrators for severe incidents. Logs must be secured against unauthorized changes. Logs must be retained for at least six (6) months.

3.3 SAFEGUARDS AGAINST UNAUTHORIZED USE AND RE-DISCLOSURE OF DATA. Requestor shall exercise due care to protect all data from unauthorized physical and electronic access. Both parties shall establish and implement the following minimum physical, electronic, and managerial safeguards for maintaining the confidentiality of information provided by either party pursuant to this Agreement:

3.3.1 Access to information provided by WADOC will be restricted to only those authorized staff, officials, and agents of the parties who need it to perform their official duties in the performance of the work requiring access to the information as detailed in this Agreement and/or contract which this Agreement concerns.

3.3.2 Requestor will store the information in an area that is safe from access by unauthorized persons during work hours as well as non-work hours, or when otherwise not in use.

3.3.3 Requestor will design, implement and maintain an information security program designed to meet at least an industry standard ability to protect the information in a manner that prevents unauthorized persons from retrieving the information by means of computer, remote terminal, or other means.

3.3.4 Requestor shall take precautions to ensure that only authorized personnel and agents are given access to files containing confidential or sensitive data.

3.3.5 Requestor shall take due care and reasonable precautions to protect WADOC Data from unauthorized physical and electronic access.

3.3.6 Both parties shall meet or exceed the requirements set forth in the OCIO's policies and standards for data security and access controls to ensure the confidentiality, availability, and integrity of all data accessed.

4. DATA SEGREGATION

4.1. WADOC Data provided pursuant to this Agreement must be segregated or otherwise distinguishable from non-WADOC Data. This requirement ensures that all WADOC Data can be identified for return or destruction upon expiration, termination, or completion of work under this Agreement. It also aids in determining whether WADOC Data has or may have been compromised in the event of a security breach.

4.2. METHODS OF DATA SEGREGATION.

4.2.1 Electronic Media. If WADOC Data is stored on electronic media (e.g., hard disk, optical disc, magnetic tape):

4.2.1.1 Such electronic media shall contain only WADOC Data; or

4.2.1.2 WADOC Data shall be stored in a partition or folder or other logical container dedicated to WADOC Data;

4.2.2 Database. If WADOC Data is stored in a database:

4.2.2.1 Such database shall contain only WADOC Data; or

4.2.2.2 WADOC Data shall be distinguishable from non-WADOC Data by the value of a specified field or fields within database records.

4.3 Paper Documents. If WADOC Data is stored as physical paper documents, such documents shall be physically segregated from non-WADOC Data and secured in a drawer, folder, or other container, with access limited to only authorized individuals.

4.3 When it is not feasible or practical to segregate WADOC Data from non-WADOC Data using the methods set forth above, then both the WADOC Data and the non-WADOC Data with which it is commingled must be protected as described for WADOC Data in this Agreement.

5. DATA CONFIDENTIALITY

5.1 Requestor acknowledges the personal or confidential nature of the information and agrees that all employees, agents, volunteers, contractors, and subcontractors with access to WADOC Data, and third parties with whom WADOC Data is shared, shall comply with all laws, regulations, and policies that apply to protection of the confidentiality of the WADOC Data. Requestor is responsible for ensuring all such employees, agents, volunteers, contractors, subcontractors, and third parties are aware of and abide by the data use and security provisions set forth in this Agreement and any amendments, attachments, or exhibits hereto. Requestor is responsible for timely providing the Department with duly executed Statements of Confidentiality and Non-Disclosure and Certifications of Data Disposition for all such employees, agents, volunteers, contractors, subcontractors, and third parties. Requestor acknowledges that the failure to meet the requirements set forth in this section is, at WADOC's discretion, cause for termination.

5.2 (Omitted.)

5.2.1 (Omitted.)

5.2.2 (Omitted.)

5.3 PENALTIES FOR UNAUTHORIZED DISCLOSURE OF INFORMATION.

In the event Requestor fails to comply with any material term of this Agreement, WADOC shall have the right to take any and all actions to remedy such failure and its effects that WADOC, in its sole discretion, deems reasonable under the circumstances. Any costs, fees, or expenses, including legal costs, incurred by WADOC as a result of Requestor's failure to comply with the terms of this Agreement shall be recoverable from Requestor. The exercise of remedies pursuant to this paragraph shall be in addition to all sanctions provided by law and to legal remedies available to parties injured by unauthorized disclosure.

6. INCIDENT NOTIFICATION AND RESPONSE

6.1 The compromise or potential compromise of WADOC Data that may be a breach that requires notice to affected individuals under RCW 42.56.590, RCW 19.255.010, or any other applicable breach notification law or rule must be reported to the WADOC Contract Manager and WADOC Chief Information Security Officer in writing within one (1) business day of discovery.

6.2 If Requestor does not have full details about the incident, it will report what information it has and provide full details as soon as possible but no later than ten (10) business days after the date of discovery. To the extent possible, these initial reports must include at least:

6.2.1 The nature of the unauthorized use or disclosure, including a brief description of the event of unauthorized use or disclosure, the date of the event, and the date of discovery.

6.2.2 A description of the types of information involved.

6.2.3 The investigative and remedial actions Requestor or its subcontractor took or will take to prevent and mitigate harmful effects and protect against recurrence.

6.2.4 Any details necessary for a determination of whether the incident is a breach that requires notification under RCW 19.255.010, RCW 42.56.590, or any other applicable breach notification law or rule.

6.2.5 Any other information WADOC reasonably requests.

6.3 As soon as reasonably practicable, Requestor must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law or WADOC.

6.4 If, in the sole judgment of WADOC, notifications to individuals must be made, Requestor will further cooperate and facilitate notification to required parties, which may include notification to affected individuals, the media, the Attorney General's Office, or other authorities based on applicable law.

At WADOC's discretion, Requestor may be required to directly fulfill notification requirements, or if WADOC elects to perform the notifications, Requestor must reimburse WADOC for all associated costs.

6.5 Requestor is responsible for all costs incurred in connection with a security incident, privacy breach, or potential compromise of WADOC Data, including, but not limited to:

6.5.1 Computer forensics assistance to assess the impact of a data breach, determine root cause, and help determine whether and the extent to which notification must be provided to comply with breach notification laws.

6.5.2 Notification and call center services for individuals affected by a security incident or privacy breach, including fraud prevention, credit monitoring, and identity theft assistance.

6.5.3 Regulatory defense, fines, and penalties from any claim in the form of a regulatory proceeding resulting from a violation of any applicable privacy or security laws or regulations.

6.6 Requestor's obligations regarding incident notification survive the termination of this Agreement and continue for as long as Requestor maintains WADOC Data and for any breach or potential breach, at any time.

7. DISPOSITION OF DATA

7.1 TIME OF DISPOSAL. Requestor shall immediately dispose of WADOC Data upon: (a) the expiration of the Agreement; (b) the termination of the Agreement; (c) the completion of work that required the data; and (d) one (1) year from the date the WADOC Data was made available to Requestor.

7.2 METHOD OF DISPOSAL. At WADOC's option, the disposal required in this section may be accomplished by the destruction of WADOC Data, the return of WADOC Data to WADOC, or a combination of both. Requestor shall perform all other actions WADOC determines necessary to protect WADOC Data. If WADOC does not specify a preferred method of disposal, Requestor shall destroy the WADOC Data.

7.3 (Omitted.)

7.4 METHODS OF DESTRUCTION.

7.4.1 Paper Documents.

7.4.1.1 Paper documents containing Category 3 data may be recycled by a contracted recycling firm, provided that the contract ensures the confidentiality of the data will be protected. Such documents may also be destroyed by on-site shredding, pulping, or incineration.

7.4.1.2 Paper documents containing Category 4 data shall be destroyed by on-site shredding, pulping, or incineration.

7.4.2 Optical Discs. Optical discs containing Category 3 or Category 4 data shall be destroyed by on-site incineration, shredding, or complete defacement of the readable surface with a coarse abrasive.

7.4.3 Magnetic Tapes. Magnetic tapes containing Category 3 or Category 4 data shall be destroyed by incineration, crosscut shredding, or degaussing.

7.4.4 Server and Workstation Hard Drives. Category 3 and Category 4 data stored on server and workstation hard drives, and other similar media, shall be destroyed by a data erasure or sanitation utility that overwrites the data at least three (3) times using either random or single character data, the degaussing of the hard drive or media sufficient to ensure that the data cannot be retrieved or reconstructed, or the complete physical destruction of the hard drive or media such that the content cannot be retrieved or reconstructed.

7.4.5 Portable Media. Category 3 and Category 4 data stored on portable media shall be destroyed by a data erasure or sanitation utility that overwrites the data at least three (3) times using either random or single character data, the complete degaussing of the portable media sufficient to ensure that the data cannot be retrieved or reconstructed, or the complete physical destruction of the portable media such that the content cannot be retrieved or reconstructed.

7.4.6 The requirements of this section shall survive the termination or expiration of this Agreement and any subsequent agreement intended to supersede this Agreement.

8. OFF-SHORE PROHIBITION

8.1 Requestor must maintain all hardcopies containing WADOC Data in the United States.

8.2 Requestor may not directly or indirectly (including through subcontractors) transport or maintain any WADOC Data, hardcopy or electronic, outside the United States unless it has advance written approval from the Department.

9. ON-SITE OVERSIGHT AND RECORDS MAINTENANCE

During the term of this Agreement, WADOC may, during normal business hours and upon reasonable written notice, audit, monitor, and review Requestor's activities and processes relevant to its obligations under this Agreement to ensure compliance therewith, within the limits of Requestor's technical capabilities. Requestor agrees to provide WADOC access to information, materials, and equipment necessary to audit, monitor, and review Requestor's activities and processes. Requestor shall cooperate with WADOC in the performance of any such audit, monitor, or review of Requestor's activities and processes.

Both parties hereto shall retain all records, books, and documents related to this Agreement for six (6) years, except for data disposed of in accordance with this Agreement. The Office of the State Auditor, federal auditors, and any persons duly authorized by the parties shall have full access to and the right to examine any of these materials during the term of this Agreement.

10. RIGHTS IN DATA

Unless otherwise provided herein, this Agreement will not be construed to effect any transfer of right or license to the embodiments of the WADOC's Data, except to the limited extent necessary to carry out the responsibilities specified in the Agreement.