[INSERT CONTRACT TYPE] Agreement
[Non-Public Work]

PROJECT TITLE Prosecuting Attorney's Electronic Case Management	***EXHIBITS*** ***(List all attached exhibits - Scope of Work, Work Schedule, Payment Schedule, Renewal Options, etc.)*** Attachment A - Scope of Work Attachment B - Schedule Attachment C - Investment Summary Attachment D - Licensing and Support Agreement Attachment E- Hosting Agreement Attachment F - Information, Privacy and Security Agreement Attachment G - Business Associate Agreement
CONTRACTOR Karpel Solutions	***CITY OF REDMOND PROJECT ADMINISTRATOR*** ***(Name, address, phone #)*** City of Redmond Dawn Johnson 425-556-2179
CONTRACTOR'S CONTACT INFORMATION ***(Name, address, phone #)*** Karpel Solutions 9717 Landmark Parkway, Suite 200 St. Louis, MO 63127 (314) 892-6300 mziemianski@karpel.com	***BUDGET OR FUNDING SOURCE*** 520.41101.00410.51880 (implementation services) 100.13100.00410.51530(support services) Project # 41080901.33
CONTRACT COMPLETION DATE 5/1/2025 Includes Implementation and 3 years of support services	***MAXIMUM AMOUNT PAYABLE*** $83,420

THIS AGREEMENT is entered into on _______________, 20__ between the City of Redmond, Washington, hereinafter called "the CITY", and the above person, firm or organization, hereinafter called "the CONSULTANT".

WHEREAS, the CITY desires to accomplish the above-referenced project; and

WHEREAS, the CITY does not have sufficient staff or expertise to meet the required commitment and therefore deems it advisable and desirable to engage the assistance of a CONSULTANT to provide the necessary services for the project; and

WHEREAS, the CONSULTANT has represented to the CITY that the CONSULTANT is in compliance with the professional registration statutes of the State of Washington, if applicable, and has signified a willingness to furnish consulting services to the CITY, now, therefore,

IN CONSIDERATION OF the terms and conditions set forth below, or attached and incorporated and made a part hereof, the parties agree as follows:

1. Retention of Consultant - Scope of Work. The CITY hereby retains the CONSULTANT to provide professional services as defined in this agreement and as necessary to accomplish the scope of work attached hereto as Exhibit A and incorporated herein by this reference as if set forth in full. The CONSULTANT shall furnish all services, labor and related equipment necessary to conduct and complete the work, except as specifically noted otherwise in this agreement.

2. Completion of Work. The CONSULTANT shall not begin any work under the terms of this agreement until authorized in writing by the CITY. The CONSULTANT shall complete all work required by this agreement according to the schedule attached as Exhibit B and incorporated herein by this reference as if set forth in full. A failure to complete the work according to the attached schedule, except where such failure is due to circumstances beyond the control of the CONSULTANT, shall be deemed a breach of this agreement. The established completion time shall not be extended because of any delays attributable to the CONSULTANT, but may be extended by the CITY, in the event of a delay attributable to the CITY, or because of unavoidable delays caused by circumstances beyond the control of the CONSULTANT. All such extensions shall be in writing and shall be executed by both parties.

3. Payment. The CONSULTANT shall be paid by the CITY for satisfactorily completed work and services satisfactorily rendered under this agreement as provided in Exhibit C, attached hereto and incorporated herein by this reference as if set forth in full. Such payment shall be full compensation for work performed or services rendered and for all labor, materials, supplies, equipment, and incidentals necessary to complete the work specified in the Scope of Work attached. The CONSULTANT shall be entitled to invoice

the CITY no more frequently than once per month during the course of the completion of work and services by the CONSULTANT. Invoices shall detail the work performed or services rendered, the time involved (if compensation is based on an hourly rate) and the amount to be paid. The CITY shall pay all such invoices within 30 days of submittal, unless the CITY gives notice that the invoice is in dispute. In no event shall the total of all invoices paid exceed the maximum amount payable set forth above, if any, and the CONSULTANT agrees to perform all services contemplated by this agreement for no more than said maximum amount.

4. Changes in Work. The CONSULTANT shall make such changes and revisions in the complete work provided by this agreement as may be necessary to correct errors made by the CONSULTANT and appearing therein when required to do so by the CITY. The CONSULTANT shall make such corrective changes and revisions without additional compensation from the CITY. Should the CITY find it desirable for its own purposes to have previously satisfactorily completed work or parts thereof changed or revised, the CONSULTANT shall make such revisions as directed by the CITY. This work shall be considered as Extra Work and will be paid for as provided in Section 5.

5. Extra Work.

A. The CITY may, at any time, by written order, make changes within the general scope of the agreement in the services to be performed. If any such change causes an increase or decrease in the estimated cost of, or the time required for, performance of any part of the work or services under this agreement, whether or not changed by the order, or otherwise affects any other terms or conditions of the agreement, the CITY shall make an equitable adjustment in the (1) maximum amount payable; (2) delivery or completion schedule or both; and (3) other affected terms, and shall modify the agreement accordingly.

B. The CONSULTANT must submit any "proposal for adjustment" under this clause within 30 days from the date of receipt of the written order to make changes. However, if the CITY decides that the facts justify it, the CITY may receive and act upon a proposal submitted before final payment of the agreement.

C. Failure to agree to any adjustment shall be a dispute under the Disputes clause of this agreement, as provided in Section 13. Notwithstanding any such dispute, the CONSULTANT shall proceed with the agreement as changed.

D. Notwithstanding any other provision in this section, the maximum amount payable for this agreement shall not be increased or considered to be increased except by specific written amendment of this agreement.

6. Ownership of Work Product. Any and all documents, drawings, reports, and other work product produced by the CONSULTANT under this agreement shall become the property of the CITY upon payment of the CONSULTANT'S fees and charges therefore. The CITY shall have the complete right to use and re-use such work product in any manner deemed appropriate by the CITY, provided, that use on any project other than that for which the work product is prepared shall be at the CITY'S risk unless such use is agreed to by the CONSULTANT.

7. Independent Contractor. The CONSULTANT is an independent contractor for the performance of services under this agreement. The CITY shall not be liable for, nor obligated to pay to the CONSULTANT, or any employee of the CONSULTANT, sick leave, vacation pay, overtime or any other benefit applicable to employees of the CITY, nor to pay or deduct any social security, income tax, or other tax from the payments made to the CONSULTANT which may arise as an incident of the CONSULTANT performing services for the CITY. The CITY shall not be obligated to pay industrial insurance for the services rendered by the CONSULTANT.

8. Indemnity. The CONSULTANT agrees to hold harmless, indemnify and defend the CITY, its officers, agents, and employees, from and against any and all claims, losses, or liability, for injuries, sickness or death of persons, including employees of the CONSULTANT, or damage to property, arising out of any willful misconduct or negligent act, error, or omission of the CONSULTANT, its officers, agents, subconsultants or employees, in connection with the services required by this agreement, provided, however, that:

A. The CONSULTANT's obligations to indemnify, defend and hold harmless shall not extend to injuries, sickness, death or damage caused by or resulting from the sole willful misconduct or sole negligence of the CITY, its officers, agents or employees; and

B. The CONSULTANT's obligations to indemnify, defend and hold harmless for injuries, sickness, death or damage caused by or resulting from the concurrent negligence or willful misconduct of the CONSULTANT and the CITY, or of the CONSULTANT and a third party other than an officer, agent, subconsultant or employee of the CONSULTANT, shall apply only to the extent of the negligence or willful misconduct of the CONSULTANT.

9. Insurance. The CONSULTANT shall provide the following minimum insurance coverages:

A. Worker's compensation and employer's liability insurance as required by the State of Washington;

B. General public liability and property damage insurance in an amount not less than a combined single limit of two million dollars ($2,000,000) for bodily injury, including death, and property damage per occurrence.

C. Professional liability insurance, if commercially available in CONSULTANT's field of expertise, in the amount of two million dollars ($2,000,000) or more against claims arising out of work provided for in this agreement.

The amounts listed above are the minimum deemed necessary by the CITY to protect the CITY'S interests in this matter. The CITY has made no recommendation to the CONSULTANT as to the insurance necessary to protect the CONSULTANT'S interests and any decision by the CONSULTANT to carry or not carry insurance amounts in excess of the above is solely that of the CONSULTANT.

All insurance shall be obtained from an insurance company authorized to do business in the State of Washington. Excepting the professional liability insurance, the CITY will be named on all insurance as an additional insured. The CONSULTANT shall submit a certificate of insurance to the CITY evidencing the coverages specified above, together with an additional insured endorsement naming the CITY, within fifteen (15) days of the execution of this agreement. The additional insured endorsement shall provide that to the extent of the CONSULTANT’s negligence, the CONSULTANT’s insurance shall be primary and non-contributing as to the City, and any other insurance maintained by the CITY shall be excess and not contributing insurance with respect to the CONSULTANT’s insurance. The certificates of insurance shall cover the work specified in or performed under this agreement. No cancellation, reduction or modification of the foregoing policies shall be effective without thirty (30) days prior written notice to the CITY.

10. Records. The CONSULTANT shall keep all records related to this agreement for a period of three years following completion of the work for which the CONSULTANT is retained. The CONSULTANT shall permit any authorized representative of the CITY, and any person authorized by the CITY for audit purposes, to inspect such records at all reasonable times during regular business hours of the CONSULTANT. Upon request, the CONSULTANT will provide the CITY with reproducible copies of any such records. The copies will be provided without cost if required to substantiate any billing of the CONSULTANT, but the CONSULTANT may charge the CITY for copies requested for any other purpose.

11. Notices. All notices required to be given by either party to the other under this Agreement shall be in writing and shall be given in person or by mail to the addresses set forth in the box for the same appearing at the outset of this Agreement. Notice by mail shall be deemed given as of the date the same is deposited in the United States mail, postage prepaid, addressed as provided in this paragraph.

12. Project Administrator. The Project Administrator shall be responsible for coordinating the work of the CONSULTANT, for providing any necessary information for and direction of the CONSULTANT's work in order to ensure that it meets the requirements of this Agreement, and for reviewing, monitoring and approving the quality and quantity of such work. The CONSULTANT shall report to and take any necessary direction from the Project Administrator.

13. Disputes. Any dispute concerning questions of fact in connection with the work not disposed of by agreement between the CONSULTANT and the CITY shall be referred for resolution to a mutually acceptable mediator. The parties shall each be responsible for one-half of the mediator's fees and costs.

14. Termination. The CITY reserves the right to terminate this agreement at any time upon ten (10) days written notice to the CONSULTANT. Any such notice shall be given to the address specified above. In the event that this agreement is terminated by the City other than for fault on the part of the CONSULTANT, a final payment shall be made to the CONSULTANT for all services performed. No payment shall be made for any work completed after ten (10) days following receipt by the CONSULTANT of the notice to terminate. In the event that services of the CONSULTANT are terminated by the CITY for fault on part of the CONSULTANT, the amount to be paid shall be determined by the CITY with consideration given to the actual cost incurred by the CONSULTANT in performing the work to the date of termination, the amount of work originally required which would satisfactorily complete it to date of termination, whether that work is in a form or type which is usable to the CITY at the time of termination, the cost of the CITY of employing another firm to complete the work required, and the time which may be required to do so.

15. Non-Discrimination. The CONSULTANT agrees not to discriminate against any customer, employee or applicant for employment, subcontractor, supplier or materialman, because of race, creed, color, national origin, sex, religion, honorable discharged veteran or military status, familial status, sexual orientation, age, or the presence of any sensory, mental, or physical disability or the use of a trained dog or service animal by a person with a disability, except for a bona fide occupational qualification. The CONSULTANT understands that if it violates this provision, this Agreement may be terminated by the CITY and that the CONSULTANT may be barred from performing any services for the CITY now or in the future.

16. Compliance and Governing Law. The CONSULTANT shall at all times comply with all applicable federal, state, and local laws, rules, ordinances, and regulations. This Agreement shall be governed by and construed in accordance with the laws of the State of Washington.

17. Subcontracting or Assignment. The CONSULTANT may not assign or subcontract any portion of the services to be provided under this agreement without the express written consent of the CITY. Any sub-consultants approved by the CITY at the outset of this agreement are named on separate Exhibit attached hereto and incorporated herein by this reference as if set forth in full.

18. Non-Waiver. Payment for any part of the work or services by the CITY shall not constitute a waiver by the CITY of any remedies of any type it may have against the CONSULTANT for any breach of the agreement by the CONSULTANT, or for failure of the CONSULTANT to perform work required of it under the agreement by the CITY. Waiver of any right or entitlement under this agreement by the CITY shall not constitute waiver of any other right or entitlement.

19. Litigation. In the event that either party deems it necessary to institute legal action or proceedings to enforce any right or obligation under this agreement, the parties agree that such actions shall be initiated in the Superior Court of the State of Washington, in and for King County. The parties agree that all questions shall be resolved by application of Washington law and that parties to such actions shall have the right of appeal from such decisions of the Superior Court in accordance with the law of the State of Washington. The CONSULTANT hereby consents to the personal jurisdiction of the Superior Court of the State of Washington, in and for King County. The prevailing party in any such litigation shall be entitled to recover its costs, including reasonable attorney's fees, in addition to any other award.

20. Taxes. The CONSULTANT will be solely responsible for the payment of any and all applicable taxes related to the services provided under this agreement and if such taxes are required to be passed through to the CITY by law, the same shall be duly itemized on any billings submitted to the CITY by the CONSULTANT.

21. City Business License. The CONSULTANT has obtained, or agrees to obtain, a business license from the CITY prior to commencing to perform any services under this agreement. The CONSULTANT will maintain the business license in good standing throughout the term of this Agreement.

22. Entire Agreement. This agreement represents the entire integrated agreement between the CITY and the CONSULTANT, superseding all prior negotiations, representations or agreements, written or oral. This agreement may be modified, amended, or added to, only by written instrument properly signed by both parties hereto. These standard terms and conditions set forth above supersede any conflicting terms and conditions on any attached and incorporate exhibit. Where conflicting language exists, the CITY'S terms and conditions shall govern.

IN WITNESS WHEREOF, the parties hereto have executed this agreement as of the day and year first above written.

CONSULTANT:

____

By:___________________________
Title:_________________________

CITY OF REDMOND:

____
Angela Birney, Mayor
DATED:_________________________

ATTEST/AUTHENTICATED:

____
City Clerk, City of Redmond

APPROVED AS TO FORM:

____
Office of the City Attorney

Exhibit A

SCOPE OF WORK

The following Scope of Work represents the services required to reach the proposed solution and a successful project. Karpel Solutions will perform all work in accordance with the descriptions, scopes and specifications hereafter described. In the event of ambiguity or inconsistencies between the Master Consulting Services Agreement and any of the exhibits to the agreement, the order of precedence determining controlling terms is as follows; Information Privacy and Security Agreement, Consulting Services Agreement, Business Associate Agreement, Statement of Work, Investment Summary, Licensing and Support Agreement, Hosting Agreement.

Phase 1 Project Plan

Karpel Solutions will begin with a project kickoff meeting with designated staff from the Redmond City Prosecutor's Office and Technology Department. This meeting is where system configuration will begin with an analysis of current business practices, gap/fit analysis, interface development analysis, reporting analysis, document template gathering for conversion and formalizing schedules such as data conversion milestones, installation and training. Karpel Solutions utilizes a Project Plan in Excel that contains tasks and milestone dates to meet the agreed upon go live implementation date.

Pre-Implementation Project Kickoff Meeting

1. Karpel Solutions will begin training the agency system administrators regarding the best practices developed by implementations of other customers in Washington and throughout America.
2. Karpel Solutions will carefully listen to the system administrators and project managers as they begin documenting the application workflow which will form the basis for the configuration of PROSECUTORbyKarpel.
3. Determine and gather the documents needed for template creation.
4. Provide detailed instructions on completing a pre-implementation spreadsheet (pre-load workbook) that will be loaded into the system prior to training. This spreadsheet will contain law enforcement agencies; officers; prosecuting attorneys; defense attorneys; judges; court/docket divisions, workflow events, disposition codes and all users of the system. This spreadsheet typically contains data received from the first data conversion but can be completed by the customer.
5. Milestones will be placed into the schedule to ensure all timelines are met prior to training.
6. During the business analysis, a Fit/Gap assessment will be made and incorporated into the project timeline.
7. A communication plan will be established between Karpel Solutions and the project manager.
8. A proposed training schedule will be given to the project manager/system administrators

that will include training group assignments and training class descriptions. Training will continue for System Administrators throughout the entire timeline.

9. Karpel Solutions will review and receive contacts and any data exchange documentation for interface requirements as deemed necessary.

Karpel Solutions will provide a Project Implementation Timeline that will include scheduled meetings; required agency resources; project scope; initial implementation and training plans, and all other deliverables as determined during the project kickoff meeting.

Business Analysis and Fit/Gap Assessment

Karpel Solutions understands that most customizations to each agency will be data driven through code tables that will be prefilled as defined by each agency. System Options to enable/disable certain features and show/hide system fields will also be part of this custom implementation. It has been our experience that each agency may have different procedures that require some software customization. There may be a data element that we don't currently capture but is needed for case processing or reporting requirements.

1. Karpel Solutions, the project manager and system administrators will review current software functionality and identify areas in which software customization is required. This will be performed on a first data conversion to show how your data looks in the application.
2. The project manager and system administrators will review how case processing occurs in the application and will provide detailed explanations of all noted inadequacies.
3. Karpel Solutions will make the required software customizations, depending on the scope of the customization, at no cost to the City as we have for all other implementations. Depending on the scope of the modification, any changes to the timeframe will be mutually agreed upon by Karpel Solutions and City of Redmon.

Application and Database Installation

1. The City of Redmond will establish a secure VPN connection allowing Karpel Solutions access to the legacy server if not going hosted.
2. Karpel Solutions will install the application database and upload the second data conversion files on the agency site.
3. Karpel Solutions will upload the client remote support tool to the server. City IT has the option to install the client remote support tool, perform application testing, operating system and browser compatibility test and MS Office compatibility /document generation tests on all agency workstations

Data Exchange Interfaces

Karpel Solutions will work closely with the City IT Department and other personnel referred by the City of Redmond to build and/or modify and test data exchanges that are currently in place or are required at a future date. We expect these interfaces to be completed within the interface project timeline. However, this is based on the availability and cooperation of the other data exchange partners. Data exchanges not currently in place, but desired by the City of Redmond will be reviewed and placed into a Phase II project schedule.

Mock "go-live" System Administrator Training

1. Karpel Solutions project manager and trainer will train agency system administrators on exactly how staff will be trained upon go live within 30 days of the agency's designated go live date.
2. System administrators will be trained on preliminary data conversion (if applicable) and will include document templates and workflow configurations.

Karpel Solutions project manager and trainer will train agency system administrators on **PROSECUTORbyKarpel** to further define workflow and system configurations 30 days prior to go live. The commitment of the system administrators and project manager will determine the success of the implementation. Karpel Solutions will work closely with the system administrators and the project manager to support them during this time for a successful implementation.

Training and Go Live
Karpel Solutions will provide training to the City taking into account the operational needs of the Prosecuting Attorney's Office. Training will be provided for technical staff, system administrators, document template authors and end users

Project Timeline

The Implementation Timeline is built around the "go live" date. Specific milestones and deadline dates are worked into the plan in order to meet this date.

Deadline	Task Description	Days out
After Contract Signing	Final Contracts, Implementation Agreement signed, and Project Kickoff Meeting is scheduled. Review this schedule. Minimum Server and Workstation requirements are explained. **Assigned resources: Vendor Project Manager, customer project manager**	90
	Server & PC assessment completed, and any necessary hardware or software ordered to meet PBK Installation Prerequisites. **Assigned resources: Customer project manager and IT personnel**	80
	First 4 hr. webinar Project Kickoff meeting with System Administrators. PBK Overview Project Team is selected including Karpel Staff and Customer System Administrators. (One Customer System Administrator must be a Policy Setting Attorney). PBK Pre-load configuration is explained, and initial Document Templates are received. 4-hour workflow pre-configuration is conducted. **Assigned resources: Vendor Project Manager, customer project manager, designate system administrators**	75

	Installation of PBK on the hosted server by Karpel. Karpel Support installation and application testing on each workstation should begin at this time. **Assigned Resources: Vendor project manager, vendor technicians.**	60
	Teleconference status meeting with Karpel and agency project manager to review and finalize pre-implementation meeting timeline agreement and review progress and answer any questions regarding pre-load workbook. **Assigned resources: Vendor project manager, Customer project manager.**	60
	Teleconference status meeting with Karpel and agency project manager to review progress and answer any questions regarding pre-load workbook. Pre-load due prior to Mock go live training. **Assigned resources: Vendor project manager, customer project manager**	45
	Training Schedule is completed with assignment of all office staff to specific training sessions. The Policy Setting Attorney must attend the initial Configuration, Case Initiation and Event Entry sessions at a minimum. Training room and equipment are verified **Assigned resources: Vendor project manager, customer project manager, system administrators**.	30
	Online 4hr Mock go live Webinar - Mock go live system administrator training and document template review. Customer will receive document templates and Event Entry Configuration. Customer must validate templates for accuracy over the next two weeks. **Assigned resources: Vendor project manager/trainer, customer project manager, system administrators**.	30
	Complete installation and testing of all workstations. **Assigned resources: Vendor project manager, customer project manager, customer IT.**	5
Go Live Date	**Customer Go Live**. Karpel trainers arrive at the Training Room. Final Configuration of PBK is performed with all System Administrators present. User Training begins. Customer begins using PBK in a live state.	**Go Live**

This schedule will be modified as mutually agreed upon by Client and Karpel Solutions.

Document conversion consists of Karpel Solutions converting existing Microsoft Word®, Microsoft Works® and Corel WordPerfect® documents provided by Client up to the time of training as outlined in the Project Timeline listed above into a format that can be utilized by PbK on a best effort basis. Karpel Solutions does not support nor will convert customized macros, auto-text files or other custom programming items not a part of the ordinary functionality of Microsoft Word®, Microsoft Works® and Corel WordPerfect®

OTHER INFORMATION

Any additional work requirements outside the scope of this proposal will be presented in the form of a change order and must be approved by client prior to start of such work. No additional charges will be incurred without prior written approval from client.

GENERAL CLIENT RESPONSIBILITIES

In order for the project to be completed on time and on budget, Client shall provide at a minimum:

1. Access to client facilities, computers, servers, network infrastructure and software as deemed necessary by the Karpel Solutions project manager.
2. Access to systems and equipment as required by Karpel Solutions including:
    a. PbK application access using Karpel Solutions laptops and client's network for training.
    b. Installation of the Karpel Solutions remote support tool on all desktops executing the PbK application.
3. An authorized contact person to assist in the definition of any project unknowns and authorized to approve the completion of each task.

Phase 2- Project Plan

Karpel Solutions will work closely with the City IT Department and other personnel referred by the City of Redmond to build and test data exchanges identified below. We expect these interfaces to be completed within the interface project timeline for each interface. The City of Redmond will complete an Interface Request Form provided to Karpel Solutions for each data exchange to formulate a project timeline.

1. Law Enforcement Interface (Spillman)
PROSECUTORbyKarpel' s built in Law Enforcement transfer will be configured to receive data exchanges from your police department. Karpel Solutions sees this interface as primarily inbound charging requests that would use our Law Enforcement Transfer wizard to carefully manage the import of charging information

2. iLinx
PROSECUTORbyKarpel integrated document management can link to documents stored in 3rd Party document management systems using a common key number, such as a file number/report number/court cause number between PROSECUTORbyKarpel and the other party document management system.

3.King County District Court (eCourt)
PROSECUTORbyKarpel already has a built-in electronic Court Transfer for electronically filing with the Courts and has the ability to receive a response which includes the court filing date and case number and first appearance date using web services

Exhibit B

SCEDULE

Project Timeline

The Implementation Timeline is built around the “go live” date. Specific milestones and deadline dates are worked into the plan in order to meet this date.

Deadline	Task Description	Days out
After Contract Signing	Final Contracts, Implementation Agreement signed, and Project Kickoff Meeting is scheduled. Review this schedule. Minimum Server and Workstation requirements are explained. **Assigned resources: Vendor Project Manager, customer project manager**	90
	Server & PC assessment completed, and any necessary hardware or software ordered to meet PBK Installation Prerequisites. **Assigned resources: Customer project manager and IT personnel**	80
	First 4 hr. webinar Project Kickoff meeting with System Administrators. PBK Overview Project Team is selected including Karpel Staff and Customer System Administrators. (One Customer System Administrator must be a Policy Setting Attorney). PBK Pre-load configuration is explained and initial Document Templates are received. 4-hour workflow pre-configuration is conducted. **Assigned resources: Vendor Project Manager, customer project manager, designate system administrators**	75
	Installation of PBK on the hosted server by Karpel. Karpel Support installation and application testing on each workstation should begin at this time. **Assigned Resources: Vendor project manager, vendor technicians.**	60
	Teleconference status meeting with Karpel and agency project manager to review and finalize pre-implementation meeting timeline agreement and review progress and answer any questions regarding pre-load workbook. **Assigned resources: Vendor project manager, Customer project manager.**	60
	Teleconference status meeting with Karpel and agency project manager to review progress and answer any questions regarding pre-load workbook. Pre-load due prior to Mock go live training. **Assigned resources: Vendor project manager, customer project manager**	45

	Training Schedule is completed with assignment of all office staff to specific training sessions. The Policy Setting Attorney must attend the initial Configuration, Case Initiation and Event Entry sessions at a minimum. Training room and equipment are verified **Assigned resources: Vendor project manager, customer project manager, system administrators**.	30
	<u>Online 4hr Mock go live Webinar</u> - Mock go live system administrator training and document template review. Customer will receive document templates and Event Entry Configuration. Customer must validate templates for accuracy over the next two weeks. **Assigned resources: Vendor project manager/trainer, customer project manager, system administrators**.	30
	Complete installation and testing of all workstations. **Assigned resources: Vendor project manager, customer project manager, customer IT.**	5
Go Live Date	**<u>Customer Go Live</u>**. Karpel trainers arrive at the Training Room. Final Configuration of PBK is performed with all System Administrators present. User Training begins. Customer begins using PBK in a live state.	**<u>Go Live</u>**

This schedule will be modified as mutually agreed upon by Client and Karpel Solutions.

Exhibit C

INVESTMENT SUMMARY

Karpel Solutions will perform according to all descriptions, scopes, and specifications herein described, in consideration for payment as set forth below.

In the event of ambiguity or inconsistencies between the Consulting Services Agreement and any of the exhibits to the agreement, the order of precedence determining controlling terms is as follows; Information Privacy and Security Agreement, Consulting Services Agreement, Business Associate Agreement, Statement of Work, Investment Summary, Licensing and Support Agreement, Hosting Agreement.

Software Products/Licensing	**Qty.**	**Price**	**Total**
PROSECUTORbyKarpel	7	$2,250	$15,750
Total Software			**$15,750**

Installation Services	**Qty.**	**Price**	**Total**
SQL Database configuration	1	$1,000	$1,000
±Client Support Tool/Scanning tool install and system compatibility check	7	$50	$350
Total Installation Services			**$1,350**

Professional Services	**Qty.**	**Price**	**Total**
Project Management		no cost	$0
Online Pre-implementation Meetings (hrs.)	8	$150	$1,200
Online Mock go-live and system administrator training (hrs.)	4	$150	$600
Document Template Conversion (up to 50 documents)	1	$1,250	$1,250
Total Professional Services			**$3,050**

Onsite Training Services	**Qty.**	**Price**		**Total**
Go-Live Training days and onsite support	5	$1,200	1 trainer	$6,000
(includes system admin training and onsite support)				
Total Onsite Training Services				**$6,000**

Annual Support and Services	**Qty.**	**Price**	**Total**
PROSECUTORbyKARPEL	7	$450	$3,150
Hosted Services	7	$100	$700
Hosted eDiscovery Service	1	$875	$875

Total Annual Support Services	$4,725

Estimated Expenses - *not to exceed*	
Travel expenses include airfare, lodging ground transportation and M&E	$3,300

Total Project Cost (excluding any applicable taxes)		$34,175
*Annual Support and Services	Year 2	$4,725
*Annual Support and Services	Year 3	$4,725
Total Three-Year Cost		**$43,625**

* *Annual Support and Services cost do not include annual support cost for data exchange interfaces*

Phase 2 Cost	Qty.	Price	Total
Data Exchange Interfaces			
Law Enforcement Interface - Spillman	1	$10,000	$10,000
Interface annual support	1	$2,000	$2,000
Court Interface-eCourt	1	$10,000	$10,000
Interface annual support	1	$2,000	$2,000
iLinx integration	1	$10,000	$10,000
Interface annual support	1	$2,000	$2,000

Payment Terms

Payment schedule to be 50% of Software User Licenses due upon signed contract agreement and the remaining project cost due upon completion of implementation and training.

Client will be invoiced upon the completion of user acceptance testing for data exchanges identified in Phase 2 Cost.

Travel and Expense Reimbursement

City agrees to reimburse travel expenses incurred by Karpel within the then current GSA guidelines for lodging and per diem rates for King County, Washington. Karpel shall use reasonable effort to obtain the lowest available travel fares. The reimbursement of travel expense is limited to directly associated expenses for airfare, lodging, meals, airport parking, car rental and airport transportation. All expenses, with the exception of meals and incidentals, will be reimbursed at actual cost and require the submittal of an original receipt attached to the invoice. Receipts will be annotated with the person's name incurring the expense. Meals and incidentals will be invoiced at per diem rates for workdays and travel days as defined in the GSA guidelines. The City will not reimburse for travel hours. Travel expenses will be itemized on the invoice per individual incurring the expense.

Exhibit D

Karpel Solutions
Licensing and Support Terms

PROSECUTOR by KARPEL

PROSECUTORbyKarpel®

LICENSE TERMS AND USE

This software, PbK is a proprietary product of Karpel Solutions. It is licensed (not sold) and is licensed to Client for its use only by the terms set forth below.

1. In consideration of payment of a sublicense fee, Karpel Solutions hereby grants Client a non-exclusive and non-transferable sublicense to use any associated manuals and/or documentation furnished.

2. Client cannot distribute, rent, sublicense or lease the software. A separate license of PbK is required for each user or employee. Each license of PbK may not be shared by more than one full time employee or user (40 hours per week), nor more than two (2) part-time employees or users, working no more than 40 hours per week together. The Client agrees that Karpel Solutions will suffer damages from the Client's breach of this term and further agrees that as such Karpel Solutions shall be entitled to the cost of the license, installation and training costs associated for each violation, including Karpel Solutions' reasonable attorneys' fees and costs.

3. License does not transfer any rights to software source codes, unless Karpel Solutions ceases to do business without transferring its duties under this agreement to another qualified software business. Karpel Solutions will, at client's expense, enter into escrow agreement for the storage of the source codes.

4. PbK and its documentation are protected by copyright and trade secret laws. Client may not use, copy, modify, or transfer the software or its documentation, in whole or in part, except as expressly provided for herein. Karpel Solutions retains all rights in any copy, derivative or modification to the software or its documentation no matter by whom made. Client shall not provide or disclose or otherwise make available PbK or any portion thereof in any form to any third party. Client agrees that unauthorized copying and distribution will cause great damage to Karpel Solutions and this damage is far greater than the value of the copies involved.

5. PbK was developed exclusively at private expense and is Karpel Solutions' trade secret. For all purposes of the Freedom of Information Act or any other similar statutory right of "open" or public records the Software shall be considered exempt from disclosure. PbK is "commercial computer software" subject to limited utilization "Restricted Rights." PbK, including all copies, is and shall remain proprietary to Karpel Solutions or its licensors.

ANNUAL SUPPORT

1. Client understands that technical support fees will be required annually, in order to receive software updates and technical support. The support period shall begin from the date of go-live as part of the initial first year costs. The Client may elect to purchase subsequent annual support, on a yearly basis at a fixed cost, and billed annually as referenced in Exhibit C – Investment Summary. The option to purchase annual support is solely at the Client's discretion. The Client's license to use PbK is not dependent upon the Client purchasing annual support; however, if the Client discontinues annual support it will not be provided with updated versions of the software, unless it is purchased. Provided Client's computers, network and systems meet recommended specifications set for by Karpel Solutions and the Client is current with annual support payments then Karpel Solutions shall provide updated versions of their system and/or software as they become available during the terms of the contract. If the option for renewal is exercised, Karpel has the right to increase current pricing.

2. Karpel Solutions will provide support (e.g. software updates, general program enhancements and technical support) for all software provided, including ongoing unlimited telephone technical support problem determination, and resolution.

3. Karpel Solutions will provide technical support Monday through Friday, at a minimum of eight (8) hours a day. Technical support services shall be available between the hours of 7:00 a.m. through 9:00 p.m. Central time, via a toll-free telephone number provided. After-hours support is available as well via the same toll-free number which will reach the on-call support group.

4. Support services include the detection and correction of software errors and the implementation of all PbK program changes, updates and upgrades. Karpel Solutions shall respond to the inquiries regarding the use and functionality of the solution as issues are encountered by Authorized Users. Support to users will be provided through the remote support tool installed on the end user's computer. This tool was installed at the time of go-live allowing Karpel to provide the needed support to meet the service level agreement. If this access is not allowed support will be delayed and the service level agreement (severity levels) are no longer in place.

5. Karpel Solutions shall be responsive and timely to technical support calls/inquires made by the Client. The Client will first make support inquires through their qualified system administrators to assure the policies and business practices of the Client are enforced prior to contacting Karpel Solutions. The timeliness of the response is dependent upon the severity of the issue/support problem, as defined below:

The severity* of the issue/support problem shall determine the average problem resolution response time in any calendar month of the contract as follows:

*If the remote support tool is not installed or available all issues will fall into the general assistance and the severity levels are no longer applicable.

Severity Level 1 shall be defined as urgent situations, when the Client's production system is down and the Client is unable to use PbK, Karpel Solutions' technical support staff shall accept the Client's call for assistance at the time the Client places the initial call; however, if such staff is not immediately available, Karpel Solutions shall return the customer's call within one (1) business hour. Karpel Solutions shall resolve Severity Level 1 problems as quickly as possible, which on average should not exceed two (2) business days, unless otherwise authorized in writing by the Client.

Severity Level 2 shall be defined as critical software system component(s) that has significant outages and/or failure precluding its successful operation, and possibly endangering the customer's environment. PbK may operate but is severely restricted. Karpel Solutions' technical support staff shall accept the customer's call for assistance at the time the customer places the initial call; however, if such staff is not immediately available, Karpel Solutions shall return the Client's call within four (4) business hours. Karpel Solutions shall resolve Severity Level 2 problems as quickly as possible, which on average should not exceed three (3) business days, unless otherwise authorized in writing by the customer.

Severity Level 3 shall be defined as a minor problem that exists with PbK but the majority of the functions are still usable and some circumvention may be required to provide service. Karpel Solutions' technical support staff shall accept the Client's call for assistance at the time the customer places the initial call; however, if such staff is not immediately available, Karpel Solutions shall return the Client's call on average no later than the next business day. Karpel Solutions shall resolve Severity Level 3 problems as quickly as possible, which should not exceed the next available release of software, unless otherwise authorized in writing by the Client.

General Assistance: For general software support/helpdesk calls not covered by the above severity level descriptions, Karpel Solutions' technical support staff shall accept the Client's call for assistance at the time the Client places the initial call; however, if such staff is not immediately available, Karpel Solutions shall return the Client's call on average no later than the next business day.

KARPEL COMPUTER SYSTEMS, INC. (dba "Karpel Solutions"),
MASTER TERMS AND CONDITIONS

GENERAL TERMS

1. SOFTWARE ANOMALIES. New commercial software releases or upgrades, or any hardware and/or software owned by or licensed to Client, used in connection with Karpel Solutions services may have anomalies, performance or integration issues unknown to Karpel Solutions which can impact the timely, successful implementation of information systems. Karpel Solutions will inform the client promptly if this occurs and will attempt to analyze, correct and/or work around the anomalies or performance issues on a "best effort" basis. Karpel Solutions is not responsible for any delay or inability to complete its services if such anomalies or performance issues occur. Client is responsible for payment for all of Karpel Solutions' services at the rate stated in the proposal whether or not a successful solution is achieved.

2. SOFTWARE AUDIT. Client agrees to allow Karpel Solutions the right to audit Client's use of PbK and licenses of PbK at any time. Client will cooperate with the audit, including providing access to any books, computers, records or other information that relate to the use of PbK. Such audit will not unreasonably interfere with Client's activities. In the event that an audit reveals unauthorized use, reproduction, distribution, or other exploitation of PbK, Client will reimburse Karpel Solutions for the reasonable cost of the audit, in addition to such other rights and remedies that Karpel Solutions may have. Karpel Solutions will not conduct an audit more than once per year.

3. CLIENT ENVIRONMENT. Client is responsible for the application, operation and management of its information technology environment, including but not limited to: (a) purchasing, licensing and maintaining hardware and software; (b) following appropriate operating procedures; (c) following appropriate protective measures to safeguard the software and data from unauthorized duplication, modification, destruction or disclosure. Karpel is not responsible for the loss of data in PbK or security breaches that result in the unauthorized dissemination of data contained in PbK that is the result of Client not following appropriate operating procedures, security and protective measures.

LIMITED WARRANTIES, LIMITATION OF LIABILITY

1. INTERNET AND NETWORK. Karpel Solutions makes PbK available to Client through the Internet and/or Client's own network and systems, to the extent commercially reasonable, and subject to outages, communication and data flow failures, interruptions and delays inherent in the Internet and network communications on the Client's own network and systems. Client recognizes that problems with the Internet, including equipment, software and network failures, impairments or congestion, or the configuration of Client's own computer systems and network, may prevent, interrupt or delay Client's access to PbK. Karpel Solutions is not liable for any delays, interruptions, suspensions or unavailability of PbK attributable to problems with the Internet or the configuration of Client's computer systems or network.

2. PASSWORD PROTECTION. Access to PbK is password-protected. Karpel Solutions provides multiple authentication alternatives for access to PbK. KARPEL SOLUTIONS STRONGLY ENCOURAGES THE USE

OF STRONG PASSWORD AUTHENTICATION. Karpel Solutions is not responsible for Client's use of the PbK. Only the number of users set forth above may access the Service and Website. Client must inform their users that they are subject to, and must comply with, all of the terms of this Agreement. Client is fully responsible for the activities of Client's employees and authorized agents who access to PbK. Karpel Solutions is not liable for any unauthorized access to PbK and data or information contained therein, including without limitation access caused by failure to protect the login and password information of users.

3. SYSTEM REQUIREMENTS. Karpel Solutions provides PbK based upon the system requirements as specified by Karpel Solutions for Client. Karpel Solutions has no liability for any failure of PbK based upon Client's failure to comply with the system requirements of Karpel Solutions.

4. THIRD PARTY SOFTWARE. Karpel Solutions makes no express or implied warranties as to the quality of third party software or as to Karpel Solutions' ability to support such software on an on-going basis.

5. DISCLAIMER. THE FOREGOING WARRANTIES ARE EXCLUSIVE AND ARE MADE IN LIEU OF ALL OTHER WARRANTIES, EITHER EXPRESS AND IMPLIED, WHICH ARE HEREBY DISCLAIMED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF NONINFRINGEMENT, TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTIES ARISING OUT OF A USE IN TRADE OR COURSE OF DEALING OR PERFORMANCE. KARPEL SOLUTIONS DOES NOT WARRANT (i) THAT ACCESS TO OR USE OF ALL OR ANY PART OF PBK WILL BE CONTINUOUS, ERROR-FREE OR UNINTERRUPTED, (ii) THAT THE RESULTS ARISING OUT OF CLIENT'S USE OF PBK WILL BE ACCURATE, COMPLETE OR ERROR-FREE, OR (iii) THAT THE SERVICE, SOFTWARE, DOCUMENTATION OR WEBSITE WILL MEET CLIENT'S NEEDS.

KARPEL SOLUTIONS EMPLOYEES

Karpel Solutions has spent substantial sums of money and invested large amounts of time in recruiting, supervising and training Karpel Solutions employees. Client further agrees that it has a unique opportunity to evaluate Karpel Solutions employees' performance, and has the potential to hire Karpel Solutions employees, and further agrees that such hiring away would substantially disrupt the essence of Karpel Solutions' business and ability to provide its services for others, and as such Karpel Solutions cannot agree to such a hiring. The Client acknowledges that Karpel Solutions employees work for Karpel Solutions under a non-competition agreement; therefore, Client agrees it shall not solicit for employment or contract as an independent contractor, or otherwise hire or engage a Karpel Solutions employee during the term of this Agreement or for a period of 2 years after the completion/termination of the project, whichever is longer.

CONFIDENTIALITY

1. CONFIDENTIALITY. Neither party shall disclose or use any confidential or proprietary information of the other party. The foregoing obligations shall not apply to information which: (i) is or becomes known publicly through no fault of the receiving party; (ii) is learned by the receiving party from a third party entitled to disclose it; or (iii) is already known to the receiving party.

2. PERSONALLY IDENTIFIABLE INFORMATION. The parties recognize that certain data Client or Karpel Solutions may use in conjunction with the PbK may be confidential personally identifiable

information of third parties. Karpel Solutions shall use all best efforts to protect the confidentiality of personally identifiable information of third parties. Karpel Solutions shall have no liability for disclosure of personally identifiable information caused by Client's own negligence or misconduct.

3. DISCLOSURE REQUIRED BY LAW. In the event that any confidential or proprietary information is required to be disclosed pursuant to any law, code, regulation or court order from a court of competent jurisdiction, the receiving party shall give the disclosing party immediate written notice of such requirement and shall use its best efforts to seek or to cooperate with the disclosing party in seeking a protective order with respect to the confidential information requested.

   Karpel Solutions recognizes the Client is a municipal entity subject to the Washington State Public Records Act, Chapter 42.56 RCW, and that the Client is obligated to disclose records upon request unless a specific exemption from disclosure exists. Nothing in the Karpel Solutions Licensing and Support Terms is intended to prevent the Client's compliance with the Public Records Act, and Client shall not be liable to Karpel Solutions due to Client's compliance with any law or court order requiring the release of public records.

4. SIMILAR PROGRAMS AND MATERIALS. Provided Karpel Solutions does not violate the provisions of this section regarding confidentiality, the Agreement shall not preclude Karpel Solutions from developing for itself, or for others, programs or materials which are similar to those produced as a result of services provided to Client.

5. INJUNCTIVE RELIEF. Any breach of the confidentiality provisions of this Section will cause irreparable harm to the other party. The parties agree that the non-breaching party may enforce the provisions of this Section by seeking an injunction, specific performance, criminal prosecution or other equitable relief without prejudice to any other rights and remedies the non-breaching party may have.

<u>MISCELLANEOUS</u>

1. ELECTRONIC DOCUMENTS. To the extent possible, and under the terms required by Client, Client and Karpel Solutions may communicate by electronic means, including but not limited to electronic email, and/or facsimile documents. Both parties agree that: a signature or an identification code ("USERID") contained in an electronic document is legally sufficient to verify the sender's identity and the document's authenticity; an electronic document that contains a signature or USERID is a signed writing; and that an electronic document, or any computer printout of it, is an original when maintained in the normal course of business.

2. In the event of ambiguity or inconsistencies between the Consulting Services Agreement and any of the exhibits to the agreement, the order of precedence determining controlling terms is as follows; Information Privacy and Security Agreement, Consulting Services Agreement, Business Associate Agreement, Statement of Work, Investment Summary, Licensing and Support Agreement, Hosting Agreement.

Exhibit E

HOSTEDbyKarpel
AGREEMENT FOR

PROSECUTOR by KARPEL

HOSTEDbyKarpel®

TABLE OF CONTENTS

In the event of ambiguity or inconsistencies between the Master Consulting Services Agreement and any of the exhibits to the agreement, the order of precedence determining controlling terms is as follows; Information Privacy and Security Agreement, Consulting Services Agreement, Business Associate Agreement, Statement of Work, Investment Summary, Licensing and Support Agreement, Hosting Agreement.

1. DEFINITIONS

a. "Confidential Information" means information of either Karpel Solutions or Client which is disclosed under this Agreement in oral, written, graphic, machine recognizable, electronic, sample or any other visually perceptible form by one of us to the other, and which is considered to be proprietary or trade secret by the disclosing party. Confidential Information of Karpel Solutions expressly includes, without limitation, the Software and Documentation. The Confidential Information of Client includes, without limitation, Personally Identifiable Information and Client Content. Confidential Information shall not include information which the party receiving the information can document: (i) was in the possession of or known by it without an obligation of confidentiality prior to receipt of the information, (ii) is or becomes general public knowledge through no act or fault of the party receiving the information, (iii) is or becomes lawfully available to the receiving party from a third party without an obligation of confidentiality, or (iv) is independently developed by the receiving party without the use of any Confidential Information.

b. "Client Content" means all data, information, documents, and file Client uploads or inputs into PbK on the Service through the website, including, without limitation, Personally Identifiable Information.

c. "Enhancements" means any specific configurations or customizations to the Software, which Client may request and Karpel Solutions agrees in writing to provide.

d. "Documentation" means any operating instructions, specifications and other documentation related to the operation, description and function of PbK, the Service or Website provided by Karpel Solutions whether supplied in paper or electronic form.

e. "Intellectual Property" means any patents, patent applications, copyrights, mask works, trademarks, service marks, trade names, domain names, inventions, improvements (whether patentable or not), trade secrets, Confidential Information, moral rights, and any other intellectual property rights.

f. "Hosted" or "Hosting" means the act of providing service and access to Client Content by the Internet.

g. "Personally Identifiable Information" means any information that may be used to identify specific persons or individuals, which is collected by either Karpel Solutions or Client for use in conjunction with the use of PbK or DbK on HOSTEDbyKarpel. Personally Identifiable Information shall be considered Confidential Information.

h. "PbK" means the PROSECUTORbyKarpel criminal case management system and specifically the Client's licensed copy of PROSECUTORbyKarpel

i. "DbK" means the DEFENDERbyKarpel public defender case management system and specifically the Client's licensed copy of DEFENDERbyKarpel.

j. "Service" means the HOSTEDbyKarpel hosting platform provided by Karpel Solutions which allows internet-based hosting of the Client's licensed copy of PbK through the Website.

k. "Service Level Requirements" means the technical service levels Karpel Solutions shall meet for Services as set forth below in the Service Level Commitments for the delivery of the Services.

l. "Software" means the Client's licensed copy of the PbK application, and includes any and all updates, enhancements, underlying technology or content, law enforcement transfer interfaces, other Enhancements and any Documentation as may be provided the Client by Karpel Solutions.

m. "Website" means the content and functionality currently located at the domain www.hostedbykarpel.com on the internet, or any successor or related domain that provides access to the Software and Service

2. FEES AND TERMS

a. FEES. Client will pay Karpel Solutions $100 per year for each user that has access to the Software through the Service and Website. A total of seven (7) users of Client are authorized access to the Service under this Agreement and the aggregate document / file storage space for all users included with the hosted fee is two terabytes (2TB) of storage. Additional users can be added at any time by Client at a rate of $100 per year. If storage exceeds 2TB, any additional storage above 2TB will be billed at a flat rate of $1,000 per 1TB, per year with no additional notice provided to the Client. Client will be billed on an annual basis.

In the event Client or Karpel terminates this agreement, Client understands and agrees to pay $1,000 to Karpel Solutions for work in connection with the return of all Client Content and Confidential Information in a format agreed to by the Client.

b. TERM. The term of this Agreement shall be for (1) year and will begin upon Karpel Solutions' receipt of Client's full payment of the applicable undisputed fees for a year. Such term shall be perpetual and automatically renew for subsequent terms of equal length, unless either Karpel Solutions or Client gives notice to the other party thirty (30) days prior to the expiration of the then-current term of intent not to renew. prior to the expiration of the term, Karpel Solutions will send Client a renewal invoice, which undisputed fees must be paid in full within thirty (30) days from the date of the invoice. As provided for in the Investment Summary, Exhibit C, the initial cost associated with Hosting fees is billed at a fixed rate for the implementation year and two subsequent years. Pricing of subsequent annual terms may be subject to change at the sole discretion of Karpel Solutions, not to exceed a 3% increase annually.

c. INTEREST AND LATE FEES. Past due accounts will be charged interest on a monthly basis, calculated at one and one-half percent (1.5%) per month of the unpaid balance or the maximum rate allowable by law.

3. SERVICE LEVEL COMMITMENT

a. UPTIME. Karpel Solutions is committed to providing the Software, Website and Service in a consistent and reliable manner. Karpel Solutions will provide the Software, Website and Service to Client with a stated minimum uptime of 99.5% to Client.

b. SCHEDULED MAINTENANCE. Karpel Solutions periodically performs scheduled maintenance including but not limited to outline, preventative or emergency maintenance of the Software, Website, and/or Service. Client understands that scheduled maintenance may affect availability of the Service, Website, and/or Software. If scheduled maintenance is to be performed Karpel Solutions will provide notice to Client three (3) days prior to the scheduled maintenance. Karpel Solutions will make every effort to schedule maintenance outside of normal business hours of the client between the hours of ten (10) p.m. and five (5) a.m. Central Standard Time.

c. DATA RETENTION AND BACKUPS. As a part of the Service and Website, Karpel Solutions will maintain under this Agreement consistent, regular and validated backup both onsite and offsite of the Client Content, Confidential Information and Software. Backups occur and will be maintained pursuant to Karpel Solutions internal backup policies. Upon written request, Karpel Solutions will make available to Client a copy of Karpel Solutions' current backup policies and procedures.

d. AUDITS AND SECURITY. Karpel Solutions is committed to maintaining the security of Client Content, Confidential Information, and Software on Karpel Solutions' Service and Website. Karpel Solutions will maintain the Software, Website and Service in a secure manner subject to the Customer Obligations outlined below. Karpel Solutions will perform annual security audits of the Website and Service to ensure the integrity and security of the Website and Service. Results of the Audits and Security Policy for Karpel Solutions will be made available to Client upon written request.

e. DATA TRANSMISSION. Karpel Solutions ensures that all data transmitted to and from the Service and Website is transmitted at a minimum level of 128-bit SSL encryption using digital certificates issued by an internationally recognized domain registrar and certificate authority.

f. DATA LOCATION. Karpel Solutions will maintain the Service, Software, Client Content and Confidential Information of Client in a SAS 70/SSAE 16 certified data facility.

4. CUSTOMER OBLIGATIONS

a. PASSWORD PROTECTION. Access to the Software through the Service and Website is password-protected. Karpel Solutions provides multiple authentication alternatives for access to the Website and Software. KARPEL SOLUTIONS STRONGLY ENCOURAGES THE USE OF STRONG PASSWORD AUTHENTICATION. Karpel Solutions is not responsible for Client's use of the Service, Website or Software. Only the number of users set forth above may access the Service and Website. Client must inform their users that they are subject to, and must comply with, all of the terms of this Agreement. Client is fully responsible for the activities of Client's employees and authorized agents who access the Service and Website. Karpel Solutions is not liable for any unauthorized access to the Service and Website, including without limitation access caused by failure to protect the login and password information of users.

b. RESTRICTIONS ON USE. Client agrees to conduct all activities on the Service and Website in accordance with all applicable laws and regulations. Access to the Service, Website, Software and Documentation must be solely for Client's own internal use. Client may not (and may not allow any third party to) (i) decompile, mirror, translate, disassemble or otherwise reverse engineer any part of the Software, source code, algorithms, or underlying ideas of the Software; (ii) provide, lease, lend, subcontract, sublicense, re-publish or use for timesharing, service bureau or hosting purposes any or all of the Software or Documentation; or (iii) reproduce, modify, copy, distribute, publish, display or create derivative works of any or all of the Software or Documentation or (iv) alter, remove, or obscure any copyright, trademark or other proprietary notices or confidentiality legends on or in the Software or Documentation.

c. SUSPENSION. Karpel Solutions reserves the right to immediately suspend access to Software without notice and at any time that Karpel Solutions suspects or has reason to suspect a security, data breach or if suspension is necessary to protect its rights, Client's rights or the rights of a third party. Karpel Solutions will immediately contact Client upon suspension of the Service and Website.

5. CONFIDENTIALITY

CONFIDENTIALITY. Confidential Information may not be, directly or indirectly, copied, reproduced, or distributed by either party to the Agreement receiving the Confidential Information except to the extent necessary for the receiving party to perform under the terms of this Agreement and only for the sole benefit of the party disclosing the Confidential Information. The party to the Agreement receiving Confidential Information may not, directly or indirectly, sell, license, lease, assign, transfer or disclose the Confidential Information of the disclosing party, except as allowed under the terms of this Agreement or upon written consent of the disclosing party.

a. PERSONALLY IDENTIFIABLE INFORMATION. The parties recognize that certain data Client or Karpel Solutions may use in conjunction with the Software may be confidential Personally Identifiable Information. Karpel Solutions shall use all best efforts to protect the confidentiality of Personally Identifiable Information. Karpel Solutions shall have no liability for disclosure of Personally Identifiable Information caused by Client's own negligence or misconduct.

b. MUNICIPAL ENTITY. Karpel Solutions recognizes the Client is a municipal entity subject to the Washington State Public Records Act, Chapter 42.56 RCW, and that Client is obligated to disclose records upon request unless a specific exemption from disclosure exists. Nothing in the Agreement is intended to prevent the Client's compliance with the Public Records Act, and the Client shall not be liable to Karpel Solutions due to Client's compliance with any law or court order requiring the release of public records.

c. INJUNCTIVE RELIEF. Any breach of the confidentiality provisions of this Section will cause irreparable harm to the other party. The parties agree that the non-breaching party may enforce the provisions of this Section by seeking an injunction, specific performance, criminal prosecution or other equitable relief without prejudice to any other rights and remedies the non-breaching party may have.

6. OWNERSHIP OF INTELLECTUAL PROPERTY

a. KARPEL SOLUTIONS OWNERSHIP. Karpel Solutions retains all right, title and interest in and to the Software, Documentation, Website, Service and related Intellectual Property. Any suggestions, solutions, improvements, corrections or other contributions Client provides regarding the Software, Documentation, Website or Services will become the property of Karpel Solutions and Client hereby assigns all such rights to Karpel Solutions without charge.

b. CLIENT OWNERSHIP. Client retains all rights, title and interest in and to the Client Content, and all related Intellectual Property. Client hereby grants to Karpel Solutions and Karpel Solutions hereby accepts a non-exclusive, non-transferable, worldwide, fully-paid license to use, copy, and modify the Client Content solely to the extent necessary and for the sole purposes of providing access to the Software, Documentation, Website, and Services or otherwise complying with its obligations under this Agreement.

7. WARRANTY

a. LIMITED WARRANTY. Karpel Solutions represents and warrants it will provide the Services and Website in a professional manner by qualified personnel. Karpel Solutions represents and warrants it has the requisite power and authority to enter into and perform its obligations under this Agreement. Karpel Solutions represents and warrants that the performance by Karpel Solutions of any services described in the Agreement shall be in compliance with all applicable laws, rules and regulations. Karpel Solutions represents and warrants it will provide access to and use of the Software, Service and Website in material accordance with the Service Level Commitment outlined above. No representations or warranties as to the use, functionality or operation of the Website, Software, or Service are made by Karpel Solutions other than as expressly stated in this Agreement.

b. INTERNET. Karpel Solutions makes the Website, Software and Services available to Client through the internet to the extent commercially reasonable, and subject to outages, communication and data flow failures, interruptions and delays inherent in Internet communications. Client recognizes that problems with the Internet, including equipment, software and network failures, impairments or congestion, or the configuration of Client's computer systems, may prevent, interrupt or delay Client's access to the Service, Website or Software. Karpel Solutions is not liable for any delays, interruptions, suspensions or unavailability of the Website or Software attributable to problems with the Internet or the configuration of Client's computer systems or network.

c. SYSTEM REQUIREMENTS. Karpel Solutions provides the Services and Website based upon the system requirements as specified by Karpel Solutions for Client. Karpel Solutions has no liability for any failure of the Services or the Software based upon Client's failure to comply with the system requirements of Karpel Solutions.

d. WARRANTY LIMITATION. The warranties set forth in this Agreement do not apply if non-compliance is caused by, or has resulted from (i) Client's failure to use any new or corrected versions of the Software or Documentation made available by Karpel Solutions, (ii) use of the Software or Documentation by Client for any purpose other than that authorized in this Agreement, (iii) use of the Software or Documentation in combination with other software, data or products that are defective, incompatible with, or not authorized in writing by Karpel Solutions for use with the Software or Documentation, (iv) misuse of the Software or Documentation, (v) any malfunction of Client's software, hardware, computers, computer-related equipment or network connection, (vi) any modification of the Software not performed by or otherwise authorized by Karpel Solutions in writing, or (vii) an event of Force Majeure.

e. DISCLAIMER. THE FOREGOING WARRANTIES ARE EXCLUSIVE AND ARE MADE IN LIEU OF ALL OTHER WARRANTIES, EITHER EXPRESS AND IMPLIED, WHICH ARE HEREBY DISCLAIMED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES OF NONINFRINGEMENT, TITLE, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTIES ARISING OUT OF A USE IN TRADE OR COURSE OF DEALING OR PERFORMANCE. KARPEL SOLUTIONS DOES NOT WARRANT (i) THAT ACCESS TO OR USE OF ALL OR ANY PART OF THE SERVICE, SOFTWARE, DOCUMENTATION OR WEBSITE WILL BE CONTINUOUS, ERROR-FREE OR UNINTERRUPTED, (ii) THAT THE RESULTS ARISING OUT OF CLIENT'S USE OF THE SOFTWARE, DOCUMENTATION OR WEBSITE WILL BE ACCURATE, COMPLETE OR ERROR-FREE, OR (iii) THAT THE SERVICE, SOFTWARE, DOCUMENTATION OR WEBSITE WILL MEET CLIENT'S NEEDS.

f. EXCLUSIVE REMEDIES. If the Website, or Services provided under this Agreement does not materially comply with the requirements stated in the Limited Warranty Section outlined above, Karpel Solutions sole obligation shall be to correct or modify the Website or Services, at no additional charge. If Karpel Solutions determines it is unable to correct what is non-conforming, Client's sole remedy will be to receive a refund of the fees paid for the non-conforming or Services, even if such remedy fails of its essential purpose. You may also terminate this Agreement as set forth in the termination provision of this Agreement.

8. LIMITATION OF LIABILITY

KARPEL SOLUTIONS IS NOT RESPONSIBLE FOR ANY LOSS OF DATA, COST OF PROCUREMENT OF SUBSTITUTE GOODS, SPECIAL, INDIRECT, INCIDENTAL, EXEMPLARY, PUNITIVE, OR CONSEQUENTIAL DAMAGES ARISING OUT OF ANY BREACH OF THIS AGREEMENT, EVEN IF KARPEL SOLUTIONS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION APPLIES TO ALL CAUSES OF ACTION, WHETHER ASSERTED ON THE BASIS OF CONTRACT, TORT (INCLUDING NEGLIGENCE OR STRICT LIABILITY), STATUTE OR OTHERWISE. UNLESS OTHERWISE SPECIFICALLY STATED, ALL REMEDIES AVAILABLE UNDER THIS AGREEMENT AND ALL REMEDIES PROVIDED BY LAW, WILL BE DEEMED CUMULATIVE AND NOT EXCLUSIVE. REGARDLESS OF THE FORM OF ANY CLAIM CLIENT MAY HAVE ARISING UNDER OR RELATING TO THIS AGREEMENT, KARPEL SOLUTIONS LIABILITY FOR ANY DAMAGES SHALL NOT EXCEED THE MAXIMUM AMOUNT ALLOWED BY INSURANCE.

9. TERMINATION

a. TERMINATION. Either party may terminate this Agreement with a thirty (30) business day written notice. Either party may immediately terminate this Agreement in the event the other party (i) files for, or has filed against it, a bankruptcy petition, and such petition is not dismissed within sixty (60) days of the filing date; or (ii) ceases to conduct business in the normal course, (iii) makes an assignment for the benefit of its creditors, (iv) is liquidated or otherwise dissolved, (v) becomes insolvent or unable to pay its debts in the normal course, or (vi) has a receiver, trustee or custodian appointed for it.

b. RIGHTS AFTER EXPIRATION OR TERMINATION. Upon expiration or termination of this Agreement, Karpel Solutions will immediately terminate Client's access to and use of the Website, Documentation, and Services. Upon expiration or termination of this Agreement, each party shall immediately cease to make use of any Confidential Information received from the other party. Within thirty (30) days of written request following termination or expiration of this Agreement, Karpel Solutions shall coordinate with Client a mutual agreeable manner for the return of Client Content and Confidential Information obtained or shared during the course of the Agreement. Client understands that upon any termination or expiration of this Agreement, Client must return to Karpel Solutions (or destroy and certify such destruction in writing) any Documentation or other materials provided by Karpel Solutions, whether in written or electronic form, regarding the Website, Software or Services provided under this Agreement. Termination is not an exclusive remedy.

10. GENERAL PROVISIONS

a. ASSIGNMENT. This Agreement will inure to the benefit of and be binding upon Karpel Solutions and Client and Karpel Solutions' respective successors and assigns. Notwithstanding the foregoing, Client may not assign or otherwise transfer this Agreement or Client's rights and obligations under this Agreement without the prior written consent of Karpel Solutions, and any purported assignment or other transfer without such consent will be void and of no force or effect. Karpel Solutions may assign and /or transfer this Agreement or Karpel Solutions' rights and obligations under this Agreement at any time.

b. MODIFICATION AND WAIVER; SEVERABILITY. Any modifications of this Agreement must be in writing and signed by both parties. A waiver by either party of a term or condition will not be deemed a waiver of any other or subsequent term or condition. Should any court of competent jurisdiction determine that any term or provision of this Agreement is unenforceable, or otherwise invalid, the offending term or provision will be modified to the minimum extent necessary to render it enforceable. If such modification is not possible, the term or provision will be severed from this Agreement with the remaining terms to be enforced to the fullest extent possible under the law.

c. FORCE MAJEURE. Except for a party's payment obligations hereunder, neither party shall be deemed in default of this Agreement to the extent that performance of its obligations or attempts to cure any breach thereof are delay or prevented by reason of any act of God, government, fire, natural disaster, accident, terrorism, network or telecommunication system failure, sabotage or any other cause beyond the control of such party ("Force

Majeure"), provided that such party promptly gives the other party written notice of such Force Majeure.

d. INDEPENDENT CONTRACTORS. The parties will be deemed to have the status of independent contractors, and nothing in this Agreement will be deemed to place the parties in the relationship of employer-employee, principal-agent, or partners or joint ventures. Neither party has the authority to bind, commit or make any representations, claims or warranties on behalf of the other party without obtaining the other party's prior written approval.

e. NOTICES. Any notices provided under this Agreement will be in writing in the English language and will be deemed to have been properly given if delivered personally or if sent by (i) a recognized overnight courier, (ii) certified or registered mail, postage prepaid, return receipt requested, or (iii) facsimile, if confirmed by mail, or (iv) electronically by email. Karpel Solutions' address for such notices is set forth below. Client's address for such notices will be the address on file with Karpel Solutions as provided by Client. Such address or contact information may be revised from time to time by provision of notice as described in this Section. All notices sent by mail will be deemed received on the tenth (10th) business day after deposit in the mail. All notices sent by overnight courier will be deemed given on the next business day after deposit with the overnight courier. All notices sent by facsimile will be deemed given on the next business day after successful transmission.

Karpel Solutions
9717 Landmark Parkway, Suite 200
St. Louis, MO 63127
(314) 892-6300
mziemianski@karpel.com

f. GOVERNING LAW AND DISPUTE RESOLUTION. This Agreement is to be construed and governed by the laws of the United States and the State of Washington, without regard to conflict of law's provisions. Any dispute arising out of or in connection with this Agreement, which cannot be settled amicably between the parties must be brought exclusively in the appropriate court located in King County, Washington. If either Karpel Solutions or Client employs attorneys to enforce any rights arising out of or relating to this Agreement, the prevailing party will be entitled to recover reasonable attorneys' fees and costs.

11. ENTIRE AGREEMENT

By signing below, Client hereby agrees to the above Agreement. This document constitutes the entire agreement between Client and Karpel Solutions with respect to the subject matter discussed above. Any waiver of any provision of this Agreement will be effective only if in writing and signed by Karpel Solutions. This Agreement supersedes and replaces all prior or contemporaneous understandings or agreements, written or oral, regarding this subject matter. This Agreement will inure to the benefit of Karpel Solutions successors, assigns and licensees.

City of Redmond	**Karpel Solutions**
_______________________________ Signature	_______________________________ Signature
_______________________________ Printed Name	_______________________________ Printed Name
_______________________________ Title	_______________________________ Title
_______________________________ Date	_______________________________ Date

RFP 10672-19
City of Redmond
Prosecuting Attorney's Case Management System

Attachment D – Information Privacy and Security Agreement

This Information Privacy and Security Agreement ("IPSA") is entered into by and between the City of Redmond ("City") and [*insert name and address of contractor*] ("Contractor") as of the date last signed below (the "Effective Date") and hereby amends the attached agreement between City and Contractor (the "Underlying Agreement"). This IPSA shall apply to the extent that the provision of services by Contractor pursuant to the Underlying Agreement, for example including but not limited to, professional services, SAAS, on-premises software, and remote desktop access, involves the processing of City Data, access to City systems, or access to City Data that is subject to privacy laws.

In consideration of the mutual promises in the Underlying Agreement, this IPSA and other good and valuable consideration, the parties agree as follows:

1. Definitions.

a. "Authorized Users" means Contractor's employees, agents, subcontractors and service providers who have a need to know or otherwise access City Data to enable Contractor to perform its obligations under the Underlying Agreement or the IPSA, and who are bound in writing by confidentiality and other obligations sufficient to protect City Data in accordance with the terms and conditions of this IPSA.

b. "City Data" means any and all information that the City has disclosed to Contractor or that Contractor has created on behalf of the City pursuant to its obligations under the Underlying Agreement. For the purposes of this IPSA, City Data does not cease to be City Data solely because it is transferred or transmitted beyond the City's immediate possession, custody, or control.

c. "Data Breach" means the unauthorized acquisition, access, use, or disclosure of City Data which compromises the security or privacy of the City Data or associated City software systems.

d. "Services" means all services, work, activities, deliverables, software or other obligations provided by Contractor pursuant to the Underlying Agreement.

2. Standard of Care.

a. Contractor acknowledges and agrees that, in the course of its engagement by City, Contractor may create, receive, or have access to City Data. Contractor shall comply with the terms and conditions set forth in this IPSA in its creation, collection, receipt, access to, transmission, storage, disposal, use, and disclosure of such City Data and be responsible for any unauthorized creation, collection, receipt, access to, transmission, storage, disposal, use, or disclosure of City Data under its control or in the possession of Authorized Users.

b. Contractor further acknowledges that use, storage, and access to City Data shall be performed with that degree of skill, care, and judgment customarily accepted as sound, quality, and professional practices. Contractor shall implement and maintain safeguards necessary to ensure the confidentiality, availability, and integrity of City Data. Contractor shall also implement and maintain any safeguards required to be implemented by applicable state and federal laws and regulations.

3. User Access to City Data.

a. Contractor shall not access, use or disclose City Data in any manner that would constitute a violation of state or federal law, the terms of the Underlying Agreement, or the terms of this IPSA. Contractor may only provide access to Authorized Users who have a legitimate business need to access, use or disclose City Data in the performance of Contractor's duties to City.

b. If Contractor requires access to a City software system, then each Authorized User must have a unique sign-on identification and password for access to City Data on City systems. Authorized Users are prohibited from sharing their login credentials, and may only receive such credentials upon execution of the Authorized User Access Agreement, attached hereto as Exhibit A. Contractor shall notify City within one (1) day of the departure of any Authorized User, so that City may terminate such Authorized User's access to City software systems.

4. Use of Subcontractors or Agents.

a. Contractor may disclose City Data to a subcontractor and may allow the subcontractor to create, receive, maintain, access, or transmit City Data on its behalf, provided that Contractor obtains satisfactory assurances that the subcontractor will appropriately safeguard the information. Without limiting the generality of the foregoing, Contractor shall require each of its subcontractors that create, receive, maintain, access, or transmit City Data on behalf of Contractor to execute a written agreement obligating the subcontractor to comply with all terms of this IPSA and to agree to the same restrictions and conditions that apply to Contractor with respect to the City Data.

b. Contractor shall be responsible for all work performed on its behalf by its subcontractors and agents involving City Data as if the work was performed by Contractor.

Contractor shall ensure that such work is performed in compliance with this IPSA, the Underlying Agreement and applicable law.

5. Use, Storage, or Access to, City Data.

a. Contractor shall only use, store, or access City Data in accordance with, and only to the extent permissible under this IPSA and the Underlying Agreement. Further, Contractor shall comply with all laws and regulations applicable to City Data (for example, in compliance with the Health Insurance Portability and Accountability Act ["HIPAA"] or the FBI Criminal Justice Information Services requirements). If Contractor has access to City protected health information, then Contractor must also execute the City's Business Associate Agreement.

b. Contractor may store City Data on servers housed in datacenters owned and operated by third parties, provided the third parties have executed confidentiality agreements with Contractor. Any transmission, transportation, or storage of City Data outside the United States is prohibited except with the prior written authorization of the City.

6. Privacy.

a. Contractor represents and warrants that in connection with the Services provided by Contractor:

i. All use of City Data by Contractor shall be strictly limited to the direct purpose of performing the Services, except to the extent that City expressly grants permission in writing for such additional uses.

ii. Collection of data which identifies individuals shall be limited to the minimum required by the Services.

iii. If the Services, in whole or part, involves access or delivery of information pertaining to the City via a public-facing web site, then Contractor represents and warrants that its current privacy policy is published online, and is accessible from the same web site as any web-hosted application that is a part of the Services. Contractor's privacy policy will provide end-users with a written explanation of the personal information collected about end-users, as well as available opt-in, opt-out, and other end-user privacy control capabilities.

iv. If Contractor creates technical system log information, aggregated technical usage or traffic data, and/or statistically measured technical usage or traffic data that contains or originated (in whole or part) from City Data, then Contractor's use of such data shall be strictly limited to the direct purpose of the Services and Contractor's technical security operations and systems maintenance. Contractor is prohibited from using such data that personally identifies an individual for secondary commercial purpose (including but not limited to marketing to such individuals, or disclosing data to third parties for reasons unrelated to the primary purpose for originally collecting the data), nor may Contractor solicit consent from the identified individual to do so unless the Underlying Agreement defines a means to do so that does not unduly burden individual privacy rights.

b. Contractor shall maintain the confidentiality of City Data. Confidential information shall not be deemed to include information which (a) is or becomes publicly known through no fault of Contractor; (b) is a publicly available document; or (c) disclosure of which is required by court order or legal requirement. If disclosure of City Data is required by court order or legal requirement the Contractor shall notify City, unless such notification is prohibited by court order or legal requirement. City may take such legally available measures as it chooses to limit or prevent disclosure of the City Data.

7. Information Security. This Section 7 applies to the extent that Contractor owns, supports, or is otherwise responsible for host(s), network(s), environment(s), or technology products (including hardware or software) which may contain City Data.

a. Contractor represents and warrants that the design and architecture of Contractor's systems (including but not limited to applications and infrastructure) shall be informed by the principle of defense-depth; controls at multiple layers designed to protect the confidentiality, integrity and availability of data.

b. Contractor shall make appropriate personnel vetting/background checks, have appropriate separation of duties, and undertake other such workflow controls over personnel activities as necessary to safeguard City Data.

c. Contractor shall implement appropriate procedures to monitor and deploy security patches and prevent unintended or unauthorized system configuration changes that could expose system vulnerability or lead to a Data Breach.

d. To the extent that the Services include software that was developed, in whole or part, by Contractor, then Contractor shall ensure that all such Services were developed within a software development life cycle (SDLC) process that includes security and quality assurance roles and control process intended to eliminate existing and potential security vulnerabilities.

e. Contractor shall have appropriate technical perimeter hardening. Contractor shall monitor its system and perimeter configurations and network traffic for vulnerabilities, indicators of activities by threat actors, and/or the presence of malicious code.

f. Contractor shall have access, authorization, and authentication technology appropriate for protecting City Data from unauthorized access or modification, and capable of accounting for access to City Data. The overall access control model of Contractor systems shall follow the principal of least privileges.

g. Contractor shall collaborate with City to safeguard electronic City Data with encryption controls over such City Data both stored and in transit. Contractor shall discontinue use of encryption methods and communication protocols which become obsolete or have become compromised. All transmissions of City Data by Contractor shall be performed using a secure transfer method.

h. Contractor shall maintain a process for backup and restoration of data with a business continuity and disaster recovery plan.

i. Contractor facilities will have adequate physical protections, commensurate with leading industry practice to secure business facilities, data centers, paper files, servers, backup systems, and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability.

j. Contractor shall, at its own expense, conduct an information security and privacy risk assessment, no less than annually, in order to demonstrate, substantiate, and assure that the security and privacy standards and practices of Contractor meet or exceed the requirements set out in this IPSA. Upon written request, Contractor shall furnish City with an executive summary of the findings of the most recent risk assessment. In lieu of providing an executive summary, Contractor may provide evidence of privacy and security certification from an independent third party.

i. City reserves the right to conduct or commission additional tests, relevant to the Services, in order to supplement Contractor's assessment. Contractor shall cooperate with such effort.

ii. If the findings of the risk assessment identify either: a potentially significant risk exposure to City Data, or other issue indicating that security and privacy standards and practices of Contractor do not meet the requirements set out in this IPSA, then Contractor shall notify City to communicate the issues, nature of the risks, and the corrective active plan.

8. Data Breach Procedures and Liability.

a. Contractor shall maintain a data breach plan in accordance with the criteria set forth in Contractor's privacy and security policy and shall implement the procedures required under such data breach plan on the occurrence of a Data Breach, in compliance with the requirements of Washington's data breach notification law codified at RCW 19.255.010. Contractor shall report, either orally or in writing, to City any Data Breach involving City Data including any reasonable belief that an unauthorized individual has accessed City Data. The report shall identify the nature of the event, a list of the affected individuals and the types of data, and the mitigation and investigation efforts of Contractor. Contractor shall make the report to the City immediately upon discovery of the Data Breach, but in no event more than forty-eight (48) hours after discovery of the Data Breach. Contractor shall provide investigation updates to the City. If such Data Breach contains protected health information, as defined by HIPAA, Contractor shall comply with the breach requirements contained in the Business Associate Agreement.

b. Notwithstanding any other provision of the Underlying Agreement, and in addition to any other remedies available to the City under law or equity, Contractor shall promptly reimburse the City in full for all costs incurred by the City in any investigation, remediation or litigation resulting from any Data Breach. Contractor's duty to reimburse the City includes but is not limited to, reimbursing to the City its cost incurred in doing the following:

i. Notification to third parties whose information may have been or were compromised and to regulatory bodies, law- enforcement agencies or other entities as may be required by law or contract;

ii. Establishing and monitoring call center(s) and credit monitoring and/or identity restoration services to assist each person impacted by a Data Breach of a nature that, in City's sole discretion, could lead to identity theft; and

iii. Payment of legal fees and expenses, audit costs, fines and penalties, and other fees imposed upon the City by a regulatory agency, court of law, or contracting partner as a result of the Data Breach.

c. Upon a Data Breach, Contractor is not permitted to notify affected individuals without the express written consent of City. Unless Contractor is required by law to provide notification to third parties or the affected individuals in a particular manner, City shall control the time, place, and manner of such notification.

9. No Surreptitious Code. Contractor warrants that, to the best of its knowledge, its system is free of and does not contain any code or mechanism that collects personal information or asserts control of the City's system without City's consent, or which may restrict City's access to or use of City Data. Contractor further warrants that it will not knowingly introduce, via any means, spyware, adware, ransomware, rootkit, keylogger, virus, trojan, worm, or other code or mechanism designed to permit unauthorized access to City Data, or which may restrict City's access to or use of City Data.

10. Public Records Act. Contractor recognizes that City is a municipal entity subject to the Public Records Act, Chapter 42.56 RCW, and that City is obligated to disclose records upon request unless a specific exemption from disclosure exists. Nothing in this IPSA is intended to prevent City's compliance with the Public Records Act, and City shall not be liable to Contractor due to City's compliance with any law or court order requiring the release of public records.

11. City Control and Responsibility. City retains all ownership, title, and rights to the City Data. City has and will retain sole responsibility for: (a) all City Data; and (b) City's information technology infrastructure, including computers, software, databases, electronic systems (including database management systems) and networks, whether operated directly by City or through the use of third-party services.

12. Term and Termination.

a. Term. The term of this IPSA is the same as the term in the Underlying Agreement.

b. Termination. In addition to the termination rights in the Underlying Agreement, City may terminate this IPSA and the Underlying Agreement as follows:

i. In the event of a material breach of this IPSA by the Contractor, provided that City first sends the Contractor written notice describing the breach with reasonable specificity, including any steps that must be taken to cure the breach. If Contractor fails to cure the breach to the reasonable satisfaction of City within thirty (30) days after receipt of the written notice, this IPSA and the Underlying Agreement may be terminated at the end of the 30-day period; provided, that if a cure cannot be completed within the thirty (30) day period, the cure period shall be extended so long as Contractor shall initiate the cure within the thirty (30) day period and thereafter diligently pursue it to completion, and provided further, that the cure period shall not be extended more than ninety (90) days after receipt of the notice of the breach; or

ii. Immediately upon a Data Breach by Contractor or Contractor's Authorized Users.

c. Effect of Expiration or Termination.

i. If City terminates the Underlying Agreement or this IPSA due to a material breach or Data Breach described in Section 12.b above, City shall not be obligated to pay any early termination fees or penalties.

ii. Within thirty (30) days following the expiration or termination of the Underlying Agreement, Contractor shall return to City all City Data in a format and structure acceptable to City and shall retain no copies of such City Data, unless City requires destruction of the City Data. As applicable, Contractor shall comply with any transition service requirements described in the Underlying Agreement.

iii. Contractor is permitted to retain City Data in its backups, archives and disaster recovery systems until such City Data is deleted in the ordinary course of Contractor's data deletion practices; and all City Data will remain subject to all confidentiality, security and other applicable requirements of this IPSA and as otherwise required by law.

13. Insurance. In addition to the insurance requirements of the Underlying Agreement, Contractor will maintain at its sole cost and expense at least the following insurance covering its obligations under this IPSA.

a. Cyber Liability Insurance: With coverage of not less than Two Million Dollars ($2,000,000) in the aggregate which shall include at a minimum coverage for (i) unauthorized access, which may take the form of a "hacker attack" or a "virus" introduced by a third party or cyber extortion; (ii) crisis management, response costs and associated expenses (e.g. legal and public relations expenses); (iii) breach of the City Data; and (iv) loss of data or denial of service incidents.

b. If Contractor's Services include professional services, then Contractor shall maintain Professional Liability or Errors and Omissions Coverage of not less than Two Million Dollars ($2,000,000) per claim and in the aggregate.

c. Contractor's insurance shall be primary to any other insurance or self-insurance programs maintained by City. Contractor shall provide to City upon execution a certificate of insurance and blanket additional insured endorsement (if applicable for the Cyber Liability Insurance). Receipt by City of any certificate showing less coverage than required is not a waiver of Contractor's obligations to fulfill the requirements.

d. Upon receipt of notice from its insurer(s), Contractor shall provide City with thirty (30) days prior written notice of any cancellation of any insurance policy, required pursuant to this Section 13. Contractor shall, prior to the effective date of such cancellation, obtain replacement insurance policies meeting the requirements of this Section 13. Failure to provide the insurance cancellation notice and to furnish to City replacement insurance policies meeting the requirements of this Section 13 shall be considered a material breach of this IPSA.

e. Contractor's maintenance of insurance as required by this Section 13 shall not be construed to limit the liability of Contractor to the coverage provided by such insurance, or otherwise limit the City's recourse to any remedy available at law or equity. Further, Contractor's maintenance of insurance policies required by this IPSA shall not be construed to excuse unfaithful performance by Contractor.

14. Cumulative Rights and Remedies. All City rights and remedies set out in this IPSA are in addition to, and not instead of, other remedies set out in the Underlying Agreement, irrespective of whether the Underlying Agreement specifies a waiver, limitation on damages or liability, or exclusion of remedies. The terms of this IPSA and the resulting obligations and liabilities imposed on Contractor shall supersede any provision in the Underlying Agreement purporting to limit Contractor's liability or disclaim any liability for damages arising out of Contractor's breach of this IPSA.

15. Indemnification. Contractor shall indemnify, defend and hold harmless City and City's officers, directors, employees, volunteers and agents (each, a "City Indemnitee") from and against any and all third party loss, cost, expense, claims, suit, cause of action, proceeding, damages or liability incurred by such City Indemnitee arising out of or relating to (i) a breach of this IPSA by Contractor; (ii) a violation by Contractor of any information security and privacy statute or regulations; or (iii) any Data Breach by Contractor.

16. Miscellaneous.

a. Order of Precedence. This IPSA shall survive the expiration or earlier termination of the Underlying Agreement. In the event the provisions of this IPSA conflict with any provision of the Underlying Agreement, or Contractor's warranties, support contract, or service level agreement, the provisions of this IPSA shall prevail.

b. Entire Agreement. This IPSA, including its exhibits, constitutes the sole and entire agreement of the Parties with respect to the subject matter of this IPSA and supersedes all prior and contemporaneous understandings, agreements, representations and warranties, both written and oral, with respect to such subject matter.

c. No Third-Party Beneficiaries. This IPSA is for the sole benefit of the parties hereto and their respective permitted successors and permitted assigns and nothing herein, express or implied, is intended to or shall confer upon any other person any legal or equitable right, benefit or remedy of any nature whatsoever under or by reason of this IPSA.

d. Notices. All notices required to be given by either party to the other under this IPSA shall be given to the Technology and Information Systems Service Desk at the following email address: servicedesk@redmond.gov, or phone number: 425-556-2929. All other notices shall be governed by the requirements of the Underlying Agreement.

e. Amendment and Modification; Waiver. No amendment to or modification of this IPSA is effective unless it is in writing, identified as an amendment to or modification of this IPSA and signed by an authorized representative of each party. The waiver of any breach of any provision of this IPSA will be effective only if in writing. No such waiver will operate or be construed as a waiver of any subsequent breach.

f. Severability. If a provision of this IPSA is held invalid under any applicable law, such invalidity will not affect any other provision of this IPSA that can be given effect without the invalid provision. Further, all terms and conditions of this IPSA will be deemed enforceable to the fullest extent permissible under applicable law and, when necessary, the court is requested to reform any and all terms or conditions to give them such effect.

g. Governing Law; Submission to Jurisdiction. This IPSA is governed exclusively by the laws of the State of Washington, excluding its conflicts of law rules. Exclusive venue for any action hereunder will lie in the state and federal courts located in Seattle, King County, Washington and both parties hereby submit to the jurisdiction of such courts.

h. Counterparts. This IPSA may be executed in counterparts and by facsimile or electronic pdf, each of which is deemed an original, but all of which together are deemed to be one and the same agreement. A signed copy of this IPSA delivered by facsimile, e-mail or other means of electronic transmission is deemed to have the same legal effect as delivery of an original signed copy of this IPSA.

[Signature Page to Follow]

IN WITNESS WHEREOF, the parties hereto have executed this agreement as of the date first above written.

Contractor

____

____

By: __________________________

Name: ________________________

Title: ________________________

Date: ________________________

City of Redmond

By: ___________________________

Name: ________________________

Title: _________________________

Date: _________________________

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement ("Agreement") is entered into by and between the City of Redmond ("Covered Entity") and _______________, ("Business Associate"), effective as of the ___ day of _______________, 20__ ("Effective Date").

RECITALS

WHEREAS, the parties contemplate one (1) or more arrangements (collectively, the "Arrangement") whereby Business Associate provides services to Covered Entity, and Business Associate creates, receives, maintains, transmits, or has access to Protected Health Information in order to provide those services;

WHEREAS, Covered Entity is subject to the Administrative Simplification requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and regulations promulgated thereunder, including the Standards for Privacy and for Security of Individually Identifiable Health Information codified at 45 Code of Federal Regulations ("CFR") Parts 160, 162, and 164 ("Privacy Regulations" and "Security Regulations");

WHEREAS, the Privacy Regulations and Security Regulations require Covered Entity to enter into a contract with Business Associate in order to mandate certain protections for the privacy and security of Protected Health Information, and those regulations prohibit the Disclosure or Use of Protected Health Information by or to Business Associate if such a contract is not in place;

AGREEMENT

NOW, THEREFORE, in consideration of the foregoing, and for other good and valuable consideration, the receipt and adequacy of which is hereby acknowledged, the parties agree as follows:

I. DEFINITIONS

1.1 Capitalized terms used but not otherwise defined in this Agreement shall have the same meaning assigned to such terms in HIPAA, as amended by the Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH Act") and as set forth in 45 CFR Parts 160, 162 and 164.

II. OBLIGATIONS OF BUSINESS ASSOCIATE

2.1 <u>Permitted Uses and Disclosures of PHI</u>. Except as otherwise limited in this Agreement, Business Associate may Use and Disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the written documents describing the Arrangement entered into by the parties, provided that such Use or Disclosure of PHI would not violate the Privacy Regulations or Security Regulations if done by Covered Entity. Business Associate further agrees not to Use or Disclose PHI other than as permitted or required by this Agreement, or as Required by Law.

2.2 Adequate Safeguards for PHI. Business Associate shall implement and maintain appropriate safeguards to prevent the Use or Disclosure of PHI in any manner other than as permitted by this Agreement or as Required by Law.

2.3 Adequate Safeguards for EPHI. Business Associate shall implement and maintain administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any EPHI that it creates, receives, maintains, or transmits on behalf of Covered Entity. Business Associate shall comply with the Security Regulations, where applicable, with respect to EPHI to prevent the Use or Disclosure of EPHI other than as permitted by this Agreement. Such compliance shall include but not be limited to, creation and maintenance of security policies and procedures pursuant to 45 CFR 164.316 and an ongoing risk assessment conducted in accordance with 45 CFR 164.308.

2.4 Reporting Non-Permitted Use, Disclosure, or Breach.

(a) Business Associate shall immediately in writing notify Covered Entity of any Use or Disclosure of PHI not permitted by this Agreement of which Business Associate becomes aware.

(b) Business Associate shall report to Covered Entity any Security Incident of which it becomes aware as follows: (a) reports of successful unauthorized access shall be made immediately; and (b) reports of attempted unauthorized access shall be made in a reasonable time and manner considering the nature of the information to be reported.

(c) Business Associate shall report to Covered Entity a Breach or potential Breach of Unsecured PHI without unreasonable delay, but not later than five (5) days, following Business Associate's discovery of such Breach or potential Breach, where such report will include the identification of each individual whose Unsecured PHI has been or is reasonably believed to have been breached, additional information that Covered Entity is required to include in a Breach notification pursuant to 45 CFR 164.404(c), and other information as requested by Covered Entity. Business Associate agrees to not notify patients, the media, or HHS of a Breach unless requested to do so by Covered Entity or unless otherwise required by law. For purposes of the foregoing obligation, "Breach" shall mean the acquisition, access, Use, or Disclosure of PHI in a manner not permitted under the HIPAA Privacy Regulations which compromises the security or privacy of such information, as further defined in 45 CFR 164.402. Business Associate shall supplement its report(s) if the above information is not available at the time of the initial report, and Business Associate shall otherwise cooperate with Covered Entity's requests for information as may be necessary for Covered Entity to evaluate the scope of the incident and related compliance issues. Business Associate must notify Covered Entity of the Breach or potential Breach regardless of whether Business Associate has conducted a risk assessment, or the results of the risk assessment, described in 45 CFR 164.404.

2.5 Notice. All reporting pursuant to this Agreement shall be to the City of Redmond Privacy Officer at the following e-mail address: privacy@redmond.gov.

2.6 Availability of Internal Practices, Books and Records to Government Agencies. Business Associate agrees to make its internal practices, books, and records relating to the Use and Disclosure of PHI by Business Associate on behalf of Covered Entity available to the Secretary of the federal Department of Health and Human Services ("HHS") for purposes of determining Covered Entity's compliance with the Privacy Regulations and Security Regulations. Business Associate shall immediately in writing notify Covered Entity of any requests made by HHS and provide Covered Entity with copies of any documents produced in response to such request.

2.7 Access to and Amendment of PHI. In the event that Covered Entity's PHI in the Business Associate's possession constitutes a Designated Record Set, Business Associate shall within five (5) days of receiving a request from Covered Entity for access to PHI about an Individual contained in a Designated Record Set, Business Associate shall: (a) make the PHI specified by Covered Entity available to Covered Entity to access and copy that PHI, and (b) make PHI available to Covered Entity for the purpose of amendment and incorporating such amendments into the PHI. Covered Entity is responsible for responding to Individuals' request for access to PHI and, in the event Business Associate receives such requests directly from Individuals, Business Associate shall notify Covered Entity of the request promptly, but in no event longer than five (5) business days, for Covered Entity to respond to the Individuals. Business Associate shall have a process in place for requests and amendments from Covered Entity.

2.8 Accounting of Disclosures.

(a) In accordance with 45 CFR 164.528, and Section 13405(c) of Title XII, Subtitle D of the HITECH Act, codified at 42 U.S.C. § 17932, Business Associate agrees to: (a) document Disclosures of PHI and information related to such Disclosures; (b) provide such documentation to Covered Entity in a time and manner designated by Covered Entity; and (c) permit Covered Entity to respond to a request by an individual for an accounting of Disclosures of PHI. Within ten (10) days of Business Associate receiving a request from Covered Entity, Business Associate shall provide to Covered Entity an accounting, as described in 45 CFR 164.528, of each Disclosure of PHI made by Business Associate or its employees, agents, representatives, or subcontractors. Covered Entity is responsible for responding to Individuals' request for an accounting and, in the event Business Associate receives such requests directly from Individuals, Business Associate shall notify Covered Entity of the request promptly, but in no event longer that five (5) business days, for Covered Entity to respond to the Individuals.

(b) Any accounting provided by Business Associate under this Section 2.8 shall include: (i) the date of Disclosure; (ii) the name, and address, if known, of the entity or person who received the PHI; (iii) a brief description of Disclosed PHI; and (iv) a brief statement of the purpose of Disclosure. For each Disclosure that could require an accounting under this Section 2.8, Business Associate shall document the information specified in (i) through (iv), above, and shall securely retain this documentation for six (6) years from the date of Disclosure.

2.9 Use of Subcontractors and Agents.

(a) Business Associate may Disclose PHI to a subcontractor, and may allow the subcontractor to create, receive, maintain, access or transmit PHI on its behalf, provided that

Business Associate obtains satisfactory assurances that the subcontractor will appropriately safeguard the information. Without limiting the generality of the foregoing, Business Associate shall require each of its subcontractors that create, receive, maintain, access or transmit PHI on behalf of Business Associate to execute a written agreement obligating the subcontractor to comply with all terms of this Agreement and to agree to the same restrictions and conditions that apply to Business Associate with respect to the PHI. Upon request from Covered Entity, Business Associate shall provide a list of subcontractors that it has Disclosed PHI to and the nature of the Disclosed PHI.

(b) Business Associate shall terminate its agreement with any subcontractor if Business Associate knows of or discover a pattern of activity or practice of a subcontractor that constitutes a material breach or violation of the subcontractor's HIPAA obligation under the written agreement with Covered Entity Business Associate shall immediately notify Covered Entity of the termination of the subcontractor agreement if such termination resulted from a material breach or violation of the subcontractor's HIPAA obligations.

(c) Business Associate shall require the subcontractor assent in writing to the jurisdiction and laws of the United States, regardless of whether the subcontractor is a foreign entity, is performing services outside the United States, or is not otherwise subject to the jurisdiction of the United States. Business Associate hereby agrees not to transmit or store any PHI outside of the United States.

2.10 Agreement to Mitigate. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a Use or Disclosure of PHI by Business Associate in violation of the requirements of this Agreement, and to promptly communicate to Covered Entity any actions taken pursuant to this Section 2.10.

2.11 Business Associate Practices, Policies and Procedures. Business Associate represents and warrants that Business Associate's privacy and security policies and practices shall meet current standards set by applicable state and federal law for the protection of PHI including, without limitation, user authentication, data encryption, monitoring and recording of database access, internal privacy standards and a compliance plan, all designed to provide assurances that the requirements of this Agreement are met. Upon reasonable notice, Business Associate shall make its facilities, systems, books and records available to Covered Entity to monitor Business Associate's compliance with this Agreement.

2.12 Compliance with Covered Entity Obligations. To the extent Business Associate carries out Covered Entity's obligations under the Privacy Regulations and Security Regulations, Business Associate shall comply with the requirements of such regulations that apply to Covered Entity in the performance of such obligations.

2.13 HITECH Act Compliance. Business Associate will comply with the requirements of the HITECH Act, codified at 42 U.S.C. §§ 17921–17954, which are applicable to business associates, and will comply with all regulations issued by HHS to implement these referenced statutes, as of the date by which business associates are required to comply with such referenced statutes and HHS regulations.

2.14 Minimum Necessary. Business Associate shall Use or Disclose only the minimum necessary amount of PHI to accomplish the intended purpose of such Use or Disclosure.

III. OBLIGATIONS OF COVERED ENTITY

3.1 Covered Entity shall, upon request, provide Business Associate with its current notice of privacy practices adopted in accordance with the Privacy Regulations.

3.2 Covered Entity shall inform Business Associate of any revocations, amendments or restrictions in the Use or Disclosure of PHI if such changes affect Business Associate's permitted or required Uses and Disclosures of PHI hereunder.

IV. ADDITIONAL PERMITTED USES

4.1 Except as otherwise limited in this Agreement or the Arrangement, Business Associate may Use and Disclose PHI as set forth below:

(a) Use of Information for Management, Administration and Legal Responsibilities. Business Associate may Use PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate.

(b) Disclosure of Information for Management, Administration and Legal Responsibilities. Business Associate may Disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate if the Disclosure is Required by Law, or Business Associate obtains reasonable assurances from the person to whom the information is Disclosed that it will be held confidentially and Used or further Disclosed only as Required by Law or for the purpose of which it was Disclosed, and the person notifies Business Associate of any instances of which it is aware where confidentiality of the information has been breached.

V. TERM AND TERMINATION

5.1 Term and Termination. This Agreement shall commence as of the Effective Date and shall continue in effect unless and until terminated by Covered Entity under this Section 5.1. Covered Entity may terminate this Agreement, without cause or penalty, on five (5) days’ prior written notice to Business Associate. In addition, this Agreement may be terminated by Covered Entity immediately and without penalty upon written notice by Covered Entity to Business Associate if Covered Entity determines, in its sole discretion, that Business Associate has violated any material term of this Agreement. Business Associate’s obligations under Sections 2.4, 2.5, 2.7, 2.8, 2.9, 2.9(b), 2.10, 5.2, 6.3, 6.5, 6.6 and 6.10 of this Agreement shall survive the termination of this Agreement.1

5.2 Disposition of PHI upon Termination. Upon termination of this Agreement, Business Associate shall either return or destroy, in Covered Entity’s sole discretion and in accordance with any instructions by Covered Entity, all PHI maintained in any form by Business Associate or its agents and subcontractors, and shall retain no copies of such PHI unless directed to do so by Covered Entity. However, if Covered Entity determines that neither return nor destruction of PHI is feasible, Business Associate may retain PHI provided that Business Associate: (a) continues to comply with the provisions of this Agreement for as long as it retains PHI, and (b) limits further Uses and Disclosures of PHI to those purposes that make the return or destruction of PHI infeasible.

VI. GENERAL TERMS

6.1 No Third Party Beneficiaries. There are no third party beneficiaries to this Agreement.

6.2 Relationship to Agreement Provisions. In the event that a provision of this Agreement is contrary to a provision of any other agreement between the parties, the provisions of this Agreement shall control.

6.3 Indemnification. Business Associate will indemnify, hold harmless and defend Covered Entity from and against any and all claims, losses, liabilities, costs, and other expenses (including attorneys' fees) incurred as a result or arising directly or indirectly out of, or in connection with (a) any misrepresentation, breach, or non-fulfillment of any undertaking on the part of Business Associate under this Agreement; (b) any claims, demands, awards, judgments, actions, and proceedings made by any person or organization, arising out of or in any way connected with Business Associate's obligations under this Agreement; and (c) a breach of unsecured PHI caused by Business Associate or its subcontractors or agents. Without limiting the generality of the foregoing, Business Associate agrees to reimburse Covered Entity for any and all costs and expenses incurred as a result or arising directly or indirectly out of Covered Entity's compliance with the HIPAA breach notification requirements set forth at 42 U.S.C. § 17932 and 45 CFR 164.40 *et.seq.* as a result of a Breach by Business Associate, including but not limited to all costs associated with Covered Entity's obligation to notify affected Individuals, the government, and the media of a Breach and any costs for credit monitoring, as applicable or establishing a toll-free number. Any limitation of liability set forth in written agreements pertaining to the Arrangement shall not apply to this Agreement.

6.4 Insurance. Business Associate shall obtain and maintain during the term of this Agreement, and at any time in which it retains PHI, liability insurance covering common law claims, breach notification expenses, data theft, and coverage related to the violation of state or federal information privacy and security laws or regulations. The policy limits for such coverage shall not be less than $1,000,000 per claim, and $3,000,000 in the annual aggregate. Such insurance shall name Covered Entity as an additional named insured. A copy of such policy or a certificate evidencing the policy shall be provided to Covered Entity upon written request. Business Associate shall provide Covered Entity with written notice of any policy cancellation within two (2) business days of the receipt of such notice. Failure of Business Associate to maintain the insurance as required shall constitute a material breach of this Agreement, upon which Covered Entity may, after giving five (5) business days notice to Business Associate to correct such breach, immediately terminate this Agreement. Business Associate's maintenance of insurance as required by this Agreement shall not be construed to limit the liability of Business Associate to the coverage provided by such insurance, or otherwise limit Covered Entity's recourse to any remedy available at law or in equity.

6.5 Data Ownership. Business Associate acknowledges and agrees that Covered Entity owns all rights, interests, and title in and to its data, including all PHI and any de-identified data, and title shall remain vested in Covered Entity at all times. Accordingly, Business Associate hereby acknowledges and agrees that it does not have the right to engage in the sale of PHI. Business Associate shall not de-identify PHI or Use or Disclose any such de-identified information unless otherwise permitted in writing by Covered Entity.

6.6 Governing Law; Venue and Jurisdiction; Attorneys' Fees. This Agreement shall in all respects be interpreted, enforced and governed by the laws of Washington State. Venue for any action or proceeding shall be in King County, Washington. In the event of any litigation or arbitration relating to or arising out of this Agreement, the substantially prevailing party or parties shall be entitled to its cost of litigation or arbitration, and reasonable attorneys' fees, including any attorneys' fees and costs incurred in bankruptcy or insolvency proceedings or on any appeal.

6.7 Legal Compliance. The parties hereto shall comply with applicable laws and regulations governing their relationship, including, without limitation, the Privacy Regulations, the Security Regulations, and any other federal or state laws or regulations governing the privacy, confidentiality, or security of patient health information, including without limitation, the Washington Uniform Healthcare Information Act, RCW Ch. 70.02. Business Associate shall comply with applicable state and federal statutes and regulations as of the date by which business associates are required to comply with applicable statutes and regulations. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Regulations, the Security Regulations, the HITECH Act, RCW ch. 70.02 and other federal or state laws or regulations governing the privacy, confidentiality, or security of patient health information or PHI.

6.8 Amendment. Upon request by Covered Entity, Business Associate agrees to promptly enter into negotiations with Covered Entity concerning the terms of an amendment to this Agreement embodying written assurances consistent with the standards and requirements of the Privacy Regulations, Security Regulations, or other applicable laws. Covered Entity may terminate this Agreement upon thirty (30) days written notice to Business Associate in the event: (a) Business Associate does not promptly enter into negotiations to amend this Agreement when requested by Covered Entity pursuant to this Section, or (b) Business Associate does not enter into an amendment of this Agreement providing assurances regarding the safeguarding of PHI that Covered Entity, in its sole discretion, deems sufficient to satisfy the standards and requirements of the Privacy Regulations, Security Regulations, or other applicable laws.

6.9 Severability. If a provision of this Agreement is held invalid under any applicable law, such invalidity will not affect any other provision of this Agreement that can be given effect without the invalid provision. Further, all terms and conditions of this Agreement will be deemed enforceable to the fullest extent permissible under applicable law, and, when necessary, the court is requested to reform any and all terms or conditions to give them such effect.

6.10 Public Records Act. The parties acknowledge that the confidentiality provisions of the HIPAA Privacy Regulations constitute an "other statute which exempts or prohibits disclosure" under the Washington State Public Records Act (see RCW 42.56.070(1); *see also Hangartner v. Seattle*, 151 Wn.2d 439, 453 (2004)), and that the confidentiality provisions under the Privacy Regulations and this Agreement shall control. Furthermore, Business Associate shall not release any de-identified health information without first notifying and conferring with Covered Entity.

6.11 No Assignment. Neither party shall assign this Agreement without the prior written consent of the other party.

6.12 Entire Agreement. This Agreement represents the entire agreement between the parties with respect to the subject matter hereof, and supersedes all prior discussions, negotiations and agreements relating to the same subject matter, including, but not limited to other business associate agreements or agreements related to patient data and the access, use, privacy, security and confidentiality of patient data. In the event of conflict between any written or oral provision of the Arrangement and any provision of this Agreement, the applicable provisions of this Agreement shall control with respect to patient data and the access, use, privacy, security and confidentiality of patient data.

6.13 Independent Contractor. Business Associate and Covered Entity are and shall be independent contractors to one another, and nothing herein shall be deemed to cause this Agreement to create an agency, partnership, or joint venture between the parties. No acts performed, or words spoken by either party with respect to any third party, shall be binding upon the other. Any and all obligations incurred by either party in connection with the performance of any of its obligations hereunder shall be solely at that party's own risk. Each party agrees that it shall not represent itself as the agent or legal representative of the other for any purpose whatsoever.

IN WITNESS WHEREOF, the parties hereto have executed this Agreement effective as of the Effective Date.

Business Associate:

____

By: ______________________________

Print Name: ___________________________

Title: ______________________________

Dated: ______________________________

City of Redmond:

____

By: ______________________________

Print Name: ___________________________

Title: ______________________________

Dated: ______________________________