Workforce Dimensions™ Agreement

This Workforce Dimensions™ Agreement (the "Agreement") governs the provision of Kronos' Workforce Dimensions software as a service and other related offerings by Kronos Incorporated and its Participating Entities ("Kronos") to City of Redmond and its Participating Entities ("Customer"). Capitalized terms not defined within the text of the Agreement are defined in Exhibit F.

This Agreement consists of this execution page and the following exhibits, which are incorporated by reference, and which form an integral part of this Agreement:

Exhibit A: General Terms and Conditions
Attachment A-2: Professional and Educational Services Policies
Attachment A-3: Service Level Agreement
Exhibit B: Workforce Dimensions Cloud Guidelines:
Exhibit C: Success Plans
Attachment C-1: Success Plans
Attachment C-2: Support Policies
Exhibit D: Acceptable Use Policy (AUP):
Exhibit E: AtomSphere Service and Boomi Software
Attachment E-1: Boomi Flow Down Provisions
Exhibit F: Definitions
Exhibit G: Add-Ins
Attachment H: Information Privacy and Security Agreement

The description of the type, quantity, and cost of the specific offerings being ordered by Customer will be described in an Order Form, that will be mutually agreed upon and signed by the Parties pursuant and subject to this Agreement. If Implementation Services are to be delivered by Kronos, the Parties may need to execute a Statement of Work, which will set forth the scope, objectives and other business terms of the Implementation Services ordered with the Order Form. Consistent with Kronos' obligations under the Information Privacy and Security Agreement included as Exhibit H, Kronos is responsible for work performed by subcontractors who perform services or host or access Customer Data pursuant to this Agreement.

This Agreement will serve as a master agreement for the Service and its related offerings. This Agreement contemplates that Participating Entities will enter into multiple Order Forms. This approach will allow the Parties to contract for additional or diverse products or services simply by signing a mutually agreeable Order Form and SOW, if applicable, without having to renegotiate or re-execute this Agreement. When Participating Entities enter into an Order Form, they are deemed to be "Customer" for purposes of this Agreement for that Order Form. Similarly, the Kronos entity that enters into an Order Form is deemed to be "Kronos" for purposes of this Agreement for that Order Form.

Kronos Incorporated	Customer
Dated:	Dated:
By:	By:
Name:	Name:
Title:	Title:

Exhibit A: General Terms and Conditions

Article 1. Order Forms

1.1 The following commercial terms may appear on an Order Form:

a. The Application(s) included in the Service, and the other offerings being ordered by Customer
b. Billing Start Date (i.e., the date the billing of the PEPM Fees commences)
c. Initial Term (i.e., the initial billing term of the Service commencing on the Billing Start Date)
d. Renewal Term (i.e., the renewal billing term of the Service)
e. Billing Frequency (i.e., the frequency for the invoicing of the PEPM Fees such as Annual in Advance or Monthly in Arrears)
    i. "Annual in Advance" means payment is due on an annual basis with the invoice being issued upon execution of the Order Form.
    ii. "Monthly in Arrears" (usually for Implementation Services) means payment is due on a monthly basis with the invoice being issued at the end of the month.
f. Payment Terms (i.e., the amount of days in which Customer must pay a Kronos invoice)
g. Shipping Terms (i.e., FOB – Shipping Point, Prepay and Add)

1.2 The following Fees may appear on an Order Form:

a. PEPM Fees for use of the Service, including PEPM Fees for Seasonal Licenses
b. Success Plan Fees for Guided and Signature Plans
c. Implementation Services Fees (The Order Form will note if Implementation Services Fees are included in PEPM Fees.)
d. Equipment Purchase Fees
e. Equipment Rental Fees
f. KnowledgeMap™ Live Fees

1.3 The parties agree that Equipment may not be purchased under this Agreement.

Article 2. Billing

2.1 Kronos will invoice the Fees on the Billing Frequency indicated on the Order Form. For each Order Form, the billing period of the PEPM Fees will start on the Billing Start Date and will continue for the time period indicated as the Initial Term. Customer will pay the undisputed Fees on the Payment Terms and in the currency, indicated on the Order Form. Customer will send payment to the attention of Kronos at the address indicated on the applicable invoice unless the Parties have made an alternative payment arrangement (such as credit card, wire transfer, ACH payment or otherwise). Unless expressly provided in this Agreement, Customer payments are non-refundable. Unless Customer has provided Kronos with valid evidence of tax-exemption, Customer is responsible for all applicable Taxes related to the Service and other items set forth on the Order Form. Each Party is responsible to pay all costs and fees attributable to such Party pursuant to the Shipping Terms indicated on the Order Form.

2.2 At the expiration of the Initial Term, and at the expiration of each Renewal Term, the Service will automatically renew for a Renewal Term. For each Renewal Term, Kronos may increase the PEPM Fees and the KnowledgeMap Live Fees by no more than four percent (4%) over the previous year's PEPM Fees and KnowledgeMap Live Fees, for the same Applications and the same licensed quantity. Kronos will provide Customer with written notice of the amount of fee increase sixty (60) days prior to the end of any

Term and reflect these increased PEPM Fees and KnowledgeMap Live Fees in the applicable invoice for each Renewal Term.

2.3 Kronos will provide the Service to Customer during the entire Initial Term and each Renewal Term. Customer will pay for the Service for the entire Initial Term and each Renewal Term.

2.4 In addition, the Customer shall not be obligated for Kronos' performance hereunder or by any provision of this Agreement during any of the Customer's future fiscal years unless and until funds have been appropriated for each such future fiscal year. In the event that funds are not appropriated for the continuation of this Agreement, the Customer will notify Kronos in writing of such non-appropriation of funds at the earliest possible date and not later than at least thirty (30) days prior to such non appropriation. Customer acknowledges that by executing an Order Form for the Service, Customer has received fiscal appropriations for the amounts due during the Term as indicated on such Order Form. Notwithstanding anything to the contrary herein or in any Order or SOW, if Customer does not receive fiscal appropriations prior to the commencement of any Renewal Term, Customer may terminate this Agreement without penalty at the end of the then-current Term.

Article 3. Implementation Services, Professional Services and Educational Services

3.1 Implementation Services are described in a SOW that the Parties will sign or reference on a signed Order Form. These SOWs are subject to this Agreement. Implementation Services are invoiced monthly as delivered, except if otherwise indicated on an Order Form. Each Party will perform their respective obligations as outlined in a signed SOW.

3.2 While Customer may configure the Applications itself, as part of the Implementation Services as described in an SOW, Kronos may also configure the Applications. Kronos will configure the Applications based on Customer's instructions and direction. Customer is solely responsible for ensuring that the Configurations comply with Applicable Law.

3.3 Kronos may also provide Professional Services to Customer that do not require an SOW but which will be as set forth on an Order Form.

3.4 KnowledgeMap™ is included in the PEPM Fees. If included on an Order Form, Kronos will also provide a subscription to KnowledgeMap™ Live. The KnowledgeMap Live 1st Year Training will expire one (1) year from purchase. KnowledgeMap Live 5 Pack entitles Customer to add up to five (5) additional named users in a KnowledgeMap Live Subscription. KnowledgeMap Live Subscription and KnowledgeMap Live 5 Pack are coterminous with the Service and will renew with the Service, unless terminated by Customer upon at least sixty (60) days prior written notice before the start of a Renewal Term. The KnowledgeMap Live Subscription Fees will be invoiced at the commencement of each year during the Term. Customer is permitted to assign one (1) employee to each user account (or seat) included in Customer's KnowledgeMap Live subscription. The number of permitted seats will appear on the Order Form. Passwords and accounts cannot be shared by multiple users. Customer will designate one (1) named user account to act as a training administrator.

3.5 Kronos may also provide ala carte educational consulting services as Implementation Services or Professional Services as described in an SOW or Order Form.

3.6 The Kronos policies set forth in Attachment A-2 shall apply to all Implementation Services and Professional Services provided by Kronos. In the event of a conflict between the Professional Services Policies and this Agreement, the terms of this Agreement shall prevail.

Article 4. Service Level Agreement

Kronos offers the Service Level Agreement and associated SLA Credits as described in Attachment A-3. The SLA Credits are Customer's sole and exclusive remedy in the event of any Outage. Kronos remains obligated to provide the Service as otherwise described in this Agreement.

Article 5. Data, Confidentiality, Security and Privacy

Section 5.1 Data

5.1.1 Customer owns Customer Data. Customer is solely responsible for Customer Data, including ensuring that Customer Data complies with the Acceptable Use Policy and Applicable Law. Customer is solely responsible for any Claims that may arise out of or relating to Customer Data.

5.1.2 Kronos owns the Aggregated Data. Subject to the limitations under the Information Privacy and Security Agreement attached hereto as Attachment H, nothing in this Agreement will prohibit Kronos from utilizing the Aggregated Data for any purposes, provided that Kronos' use of Aggregated Data will anonymize Customer Data, will not identify Customer, will not reveal any Customer Confidential Information, and will not reveal any Personally Identifiable Information.

Section 5.2 Confidentiality

5.2.1 Each Party will treat the Confidential Information of the other Party with a reasonable standard of care commensurate with the sensitivity of such Confidential Information and as further described in this Agreement. Each Party will only use the Confidential Information of the other Party for the purposes of fulfilling its obligations under this Agreement and as reasonably necessary to provide the Service. Confidential Information may be shared with and disclosed to (i) any subsidiary or affiliate of each of the Parties, or (ii) any court or governmental agency of competent jurisdiction, as required by a legal process, including without limitation Public Records Act, Chapter 42.56 RCW, and in connection with any proceeding to establish a Party's rights or obligations under this Agreement (provided however that, when permitted by Applicable Law, a Party will give the other reasonable prior written notice so that the discloser has an opportunity to contest any disclosure required by a legal process). Either Party may seek injunctive relief to preserve its rights under this section without the requirement to post a bond.

5.2.2 Public Records Act. Kronos recognizes that Customer is a municipal entity subject to the Public Records Act, Chapter 42.56 RCW and that Customer is obligated to disclose records upon request unless a specific exemption from disclosure exists. Nothing in this Agreement is intended to prevent Customer's compliance with the Public Records Act. In the event that Customer receives a public records request under Chapter 42.56 RCW or similar law for the disclosure of information related to Kronos' Services, Software and Kronos Materials, Customer shall promptly provide written notice of such disclosure so that Kronos can take appropriate steps to protect its interest and seek the exemption as provided under the Public Records Act. Customer shall reasonably cooperate with Kronos and comply with any injunction or court order obtained by Kronos that prohibits the disclosure of any such confidential records; however,

in the event a higher court overturns such injunction or court order and such higher court action is or has become final and non-appealable, Kronos shall indemnify Customer for any fines or penalties imposed on and paid by Customer for failure to disclose such records as required hereunder (but only to the extent that such failure was a direct result of Customer's compliance with Kronos' instructions or a court order or injunction received by Kronos) within forty-five (45) days of a request from Client, unless additional time is reasonably necessary under the circumstances and is agreed to by the parties.

Section 5.3 Security and Privacy

5.3.1 Kronos will maintain the Controls throughout the Term.

5.3.2 Each Party will comply with all Applicable Laws, including, without limitation, Data Protection Laws.

5.3.3 Kronos employees will access Customer Data from the locations from which such employees work. Customer consents to Kronos' handling, collection, use, transfer, and processing of Customer Data to provide the Service. As may be required by Applicable Law, Customer will ensure that Customer Data may be provided to Kronos for the purposes of providing the Service. Customer has obtained all necessary consents from individuals to enable Kronos to use the Customer Data to provide the Service. As may be contemplated by the applicable Data Protection Laws, Customer will remain the "controller" of Customer Data and Kronos will be considered a "processor" of Customer Data.

5.3.4 As further described in the Information Privacy and Security Agreement attached hereto as Attachment H, Kronos will notify Customer in accordance with Applicable Law upon becoming aware of an unauthorized access of Customer Data. To the extent reasonably possible, such a notification will include, at a minimum (i) a description of the breach, (ii) the information that may have been obtained as a result of the breach, and (iii) the corrective action Kronos is taking in response to the breach.

5.3.5 In the event that Kronos breaches its data security obligations of section 5.3 and that failure results in the unauthorized disclosure of personally identifiable data (as defined by applicable law), Kronos shall be liable for paying for the following costs to remediate, as a required by applicable laws, any such unauthorized disclosure:

a. the reasonable cost of providing notice of the breach to individuals affected by such breach as required by applicable law, the parties acknowledging that express courier service is not reasonable in this context;
b. the reasonable cost of providing required notice of the breach to government agencies, credit bureaus, and/or other required entities as required by applicable law;
c. the cost of providing individuals affected by such breach with credit protection services designed to prevent fraud associated with identity theft crimes for a specific period not to exceed 12 months, to the extent the misuse or disclosure of the affected individual's personally identifiable data could lead to a compromise of the data subject's credit or credit standing and as required by applicable law;
d. any other fines, penalties or services required by applicable law.

In each case, to the extent the unauthorized disclosure is caused in part by Customer, the damages described above will be apportioned between Kronos and Customer on a comparative fault basis. Customer will have contributed to such breach if Customer fails to only provide Kronos with the personally identifiable data minimally required to accomplish tasks for which Customer is using the Applications.

Article 6. Warranty

Kronos warrants that the Service will be provided in a professional and workmanlike manner. TO THE EXTENT PERMITTED UNDER APPLICABLE LAW, KRONOS DISCLAIMS ALL OTHER WARRANTIES RELATED TO THE SERVICE, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. If Customer informs Kronos in writing that there is a material deficiency in the Service which is making this warranty untrue, Kronos will use its reasonable commercial efforts to correct the non-conforming Service at no additional charge, and if Kronos is unable to do so within a reasonable period of time, Customer may terminate the then remaining Term of the Agreement and provide Customer a refund of the prorated portion of the Fees applicable to the remaining Term, which will be Customer's sole and exclusive remedy. Customer agrees to provide Kronos with reasonable information and assistance to enable Kronos to reproduce or verify the non-conforming aspect of the Service.

Article 7. License

Section 7.1 Technology License

7.1.1 As part of the Service, Kronos will provide Customer access to and use of the Technology, including the Applications. Technology will include an Add-In if licensed by Customer pursuant to an Order Form. Kronos hereby grants Customer a limited, revocable, non-exclusive, non-transferable, non-assignable right to use the Service, including the Technology, during the Term and for internal business purposes only. Customer acknowledges and agrees that the right to use the Service, including Seasonal Licenses when included on the Order Form, is limited based upon the number of Authorized Users, and Customer's payment of the corresponding PEPM Fees. Customer agrees to use the Applications only for the number of employees stated on the total of all Order Forms for the applicable Applications. Customer agrees not to use any other Application nor increase the number of employees using an Application unless Customer enters into an additional Order Form that will permit the Customer to have additional Authorized Users. The license for any Add-In may be terminated by Customer at any time upon written notice to Kronos.

7.1.2 Kronos owns all title or possesses all intellectual property rights in and to the Technology used in delivering the Service. Customer has a right to use this Technology and to receive the Service subject to this Agreement. No other use of the Technology is permitted. Customer is specifically prohibited from reverse engineering, disassembling or decompiling the Technology, or otherwise attempting to derive the source code of the Technology. Customer cannot contact third party licensors or suppliers for direct support of the Technology. No license, right, or interest in any Kronos trademark, trade name, or service mark, or those of any third party supplying Technology as part of the Service, is granted hereunder.

Article 8. Scope and Authority

8.1 Participating Entities may order the Service and other related offerings from Kronos by signing an Order Form contemporaneously with this Agreement, or in the future by signing an Order Form specifically referencing this Agreement. Only the Parties entering into a particular Order Form will be responsible under this Agreement for the items on that Order Form.

8.2 The person signing this Agreement on behalf of Kronos and on behalf of Customer represent that they are lawfully able to enter into contracts and are authorized to sign this Agreement and bind the entity on

whose behalf they are entering into this Agreement. By signing an Order Form, each person signing such Order Form represents that they are lawfully able to enter into contracts and are authorized to sign the Order Form and bind the Participating Entity on whose behalf they are signing the Order Form.

8.3 Authorized Users may access the Service on Customer's behalf, and Customer will be responsible for all actions taken by its Authorized Users. Customer will make sure that Authorized Users comply with Customer's obligations under this Agreement. Unless Kronos breaches its obligations under this Agreement, Kronos is not responsible for unauthorized access to Customer's account, nor activities undertaken with Customer's login credentials, nor by Customer's Authorized Users. Customer should contact Kronos immediately if Customer believes an unauthorized person is using Customer's account or that Customer's account information has been compromised.

8.4 Use of the Service includes the ability to enter into agreements and/or to make transactions electronically. This feature of the Service is referred to as the "Marketplace". The use of the Marketplace can be configured, and Customer may disable use of the Marketplace by some or all of its Authorized Users. CUSTOMER ACKNOWLEDGES THAT WHEN AN AUTHORIZED USER INDICATES ACCEPTANCE OF AN AGREEMENT AND/OR TRANSACTION ELECTRONICALLY WITHIN THE MARKETPLACE, THAT ACCEPTANCE WILL CONSTITUTE CUSTOMER'S LEGAL AGREEMENT AND INTENT TO BE BOUND BY AND TO PAY FOR SUCH AGREEMENTS AND TRANSACTIONS. THIS ACKNOWLEDGEMENT THAT CUSTOMER INTENDS TO BE BOUND BY SUCH ELECTRONIC ACCEPTANCE APPLIES TO ALL AGREEMENTS AND TRANSACTIONS CUSTOMER ENTERS INTO THROUGH THE SERVICE, SUCH AS ORDERS, CONTRACTS, STATEMENTS OF WORK, AND NOTICES OF CANCELLATION.

Article 9. Suspension

9.1 Kronos may suspend the Service if any undisputed amount that Customer owes Kronos is more than 30 days overdue. Kronos will provide Customer with at least 7 days prior written notice that the Customer's account is overdue before Kronos suspends the Service. Upon payment in full of all overdue amounts, Kronos will immediately restore the Service.

9.2 Customer is responsible for complying with the AUP. Kronos and its third party cloud service provider reserve the right to review Customer's use of the Service and Customer Data for AUP compliance and enforcement. If Kronos discovers an AUP violation, and Kronos reasonably determines that Kronos must take immediate action to prevent further harm, Kronos may suspend Customer's use of the Service immediately without notice. Kronos will contact Customer when Kronos suspends the Service to discuss how the violation may be remedied, so that the Service may be restored as soon as possible. If Kronos does not reasonably believe it needs to take immediate action, Kronos will notify Customer of the AUP violation. Even if Kronos doesn't notify Customer or suspend the Service, Customer remains responsible for any such AUP violation. Kronos will restore the Service once the AUP violation is cured or as both Parties may agree.

Article 10. Termination

Section 10.1. Types of Termination

10.1.1 Non-renewal. Either Party may terminate the Service upon at least thirty (30) days prior written notice before the start of a Renewal Term. Customer may terminate Seasonal Licenses upon at least sixty (60) days prior written notice before the start of a Renewal Term.

10.1.2 For Cause. Either Party may terminate the Service and this Agreement if the other Party fails to perform any material obligation under this Agreement, and such Party is not able to cure the non-performance within 30 days of the date such Party is notified by the other Party of such default.

10.1.3 For Bankruptcy. If either Party: (i) becomes insolvent, (ii) makes a general assignment for the benefit of our creditors, (iii) is adjudicated as bankrupt or insolvent, or (iv) has a proceeding commenced against it under applicable bankruptcy laws, the other Party may ask for a written assurance of future performance of a Party's obligations under this Agreement. If an assurance that provides reasonable evidence of future performance is not provided within 10 business days of a written request, the requesting Party may immediately terminate this Agreement upon written notice.

Section 10.2 Effects of Termination

If the Agreement is terminated for any reason:

a. All undisputed Fees will be paid by Customer for amounts owed through the effective date of termination.
b. Any Fees paid by Customer for the Service not rendered prior to the effective date of termination will be credited against Customer's account, with any remaining amounts refunded to Customer within thirty (30) days of the effective date of termination.
c. Customer's right to use the Service will end as of the effective date of termination. Notwithstanding such termination, Customer will have thirty (30) days after the effective date of termination to access the Service for purposes of retrieving Customer Data through tools provided by Kronos that will enable Customer to so extract Customer Data. If Customer requires a longer period of access to the Service after termination to retrieve Customer Data, such access will be subject to additional Fees. Extended access and use of the Services will be subject to the terms of this Agreement.
d. Kronos will delete Customer Data after Customer's rights to access the Service and retrieve Customer Data have ended. Kronos will delete Customer Data in a series of steps and in accordance with Kronos' standard business practices for destruction of Customer Data and system backups. Final deletion of Customer Data will be completed when the last backup that contained Customer Data is overwritten.
e. Kronos and Customer will each return or destroy any Confidential Information of the other Party, with any retained Confidential Information remaining subject to this Agreement.
f. Provisions in this Agreement which by their nature are intended to survive in the event of a dispute or because their obligations continue past termination of the Agreement will so survive.

Article 11. Indemnification

11.1 Kronos will indemnify, defend and hold the Customer Indemnified Parties harmless, from and against any and all Claims alleging that the permitted uses of the Service, Technology or Applications infringe or misappropriate any legitimate copyright or patent. Kronos will indemnify, defend and hold harmless the Customer Indemnified Parties against any liabilities, obligations, costs or expenses (including, without limitation, reasonable attorneys' fees) actually awarded to a third party by a court of applicable jurisdiction as a result of such Claim, or as a result of Kronos' settlement of such a Claim. In the event that a final injunction is obtained against Customer's use of the Service by reason of infringement or misappropriation of any such copyright or patent, or if in Kronos' opinion, the Service is likely to become the subject of a successful claim of infringement or misappropriation, Kronos (at its option and expense) will use commercially reasonable efforts to either (a) procure for Customer the right to continue using the

Service as provided in the Agreement, or (b) replace or modify the Service so that the Service becomes non-infringing but remains substantively similar to the affected Service. Should neither (a) nor (b) be commercially reasonable, either Party may terminate the Agreement and the rights granted hereunder, at which time Kronos will provide a refund to Customer of the PEPM Fees paid by Customer for the infringing elements of the Service covering the period of their unavailability and Customer may pursue other remedies at law in accordance with the terms of this Agreement.

11.2 Kronos will have no liability to indemnify or defend Customer to the extent the alleged infringement or misappropriation is based on: (a) a modification of the Service undertaken by anyone other than Kronos, except when undertaken at Kronos' written direction; (b) use of the Service other than as authorized by this Agreement; or (c) use of the Service in conjunction with any equipment, service or software not provided or permissible in accordance with Documentation provided by Kronos, where the Service would not otherwise infringe, misappropriate or otherwise become the subject of the Claim.

11.4 The Indemnified Party will provide written notice to the indemnifying party promptly after receiving notice of such Claim. If the defense of such Claim is materially prejudiced by a delay in providing such notice, the purported indemnifying party will be relieved from providing such indemnity to the extent of the delay's impact on the defense. The indemnifying party will have sole control of the defense of any indemnified Claim and all negotiations for its settlement or compromise, provided that such indemnifying party will not enter into any settlement which imposes any obligations or restrictions on the applicable Indemnified Parties without the prior written consent of the other Party. The Indemnified Parties will cooperate fully (at the indemnifying party's request and expense) with the indemnifying party in the defense, settlement or compromise of any such action. The indemnified party may retain its own counsel at its own expense, subject to the indemnifying party's rights above.

Article 12. Extent and Limitations of Liability

12.1 EXCEPT FOR EITHER PARTY'S INDEMNIFICATION OBLIGATIONS EXPRESSLY SET FORTH IN THIS AGREEMENT, THE TOTAL AGGREGATE LIABILITY OF EITHER PARTY IN CONNECTION WITH THIS AGREEMENT WILL BE LIMITED TO ACTUAL AND DIRECT DAMAGES INCURRED BY SUCH PARTY, SUCH DAMAGES NOT TO EXCEED AN AMOUNT EQUAL TO TWO TIMES THE TOTAL NET PAYMENTS RECEIVED BY KRONOS FOR THE SERVICE IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE DATE IN WHICH THE CLAIM ARISES. NOTWITHSTANDING THE FOREGOING, IN THE EVENT KRONOS BREACHES ITS DATA SECURITY OBLIGATIONS OF SECTION 5.3 WHICH CAUSES THE UNAUTHORIZED RELEASE OF CUSTOMERS PERSONALLY IDENTIFIABLE DATA, THE TOTAL AGGREGATE LIABILITY OF KRONOS TO CUSTOMER IN CONNECTION WITH SUCH DATA BREACH SHALL NOT EXCEED THREE TIMES (3X) THE TOTAL NET PAYMENTS RECEIVED BY KRONOS FOR THE SERVICE IN THE TWELVE (12) MONTH PERIOD IMMEDIATELY PRECEDING THE DATE IN WHICH THE CLAIM ARISES.

12.2 **NEITHER PARTY WILL BE LIABLE FOR ANY INDIRECT, CONSEQUENTIAL, INCIDENTAL, SPECIAL, OR PUNITIVE DAMAGES.** NEITHER PARTY WILL BE LIABLE FOR THE COST OF ACQUIRING SUBSTITUTE OR REPLACEMENT SERVICES. NEITHER PARTY WILL BE LIABLE FOR ANY LOST OR IMPUTED PROFITS OR REVENUES OR LOST DATA RESULTING FROM DELAYS, NONDELIVERIES, MISDELIVERIES OR SERVICES INTERRUPTION, HOWEVER CAUSED, ARISING FROM OR RELATED TO THE SERVICE OR THIS AGREEMENT. THESE LIMITATIONS APPLY FOR ANY REASON, REGARDLESS OF ANY LEGAL THEORY AND FOR WHATEVER

REASON LIABILITY IS ASSERTED. THIS IS TRUE EVEN IF KRONOS AND CUSTOMER HAVE TOLD EACH OTHER THAT EITHER ONE IS CONCERNED ABOUT A PARTICULAR TYPE OF LIABILITY.

Article 13. Changes

The information found in any Exhibit (or at any URL referenced in this Agreement) may change over the Term. Kronos will provide Customer with sixty (60) days advance notice of such change and any such change will be effective as of the start of the next Renewal Term after such change is announced or published by Kronos. In Customer's sole discretion, Customer may terminate the Services for convenience in the event Kronos makes a change to any Exhibit that materially degrades or changes the Services.

Article 14. Feedback

From time to time, Customer may provide Feedback. Kronos has sole discretion to determine whether or not to undertake the development of any enhancements, new features or functionality contained in or with Feedback. Customer hereby grants Kronos a royalty-free, fully paid up, worldwide, transferable, sublicensable, irrevocable, perpetual license to use, copy, distribute, transmit, display, perform, create derivative works of and otherwise fully exercise and commercially exploit the Feedback for any purpose in connection with Kronos' business without any compensation to Customer or any other restriction or obligation, whether based on intellectual property right claim or otherwise. For the avoidance of doubt, no Feedback will be deemed to be Customer Confidential Information, and nothing in this Agreement limits Kronos' right to independently use, develop, evaluate, or market products or services, whether incorporating Feedback or otherwise.

Article 15. General

15.1 This Agreement is governed by and is to be interpreted in accordance with the laws of the state of Washington, without regard to any conflict of law provision if and as applicable. Exclusive venue for any action hereunder will lie in King County Superior Court. Each Party waives the application of the United Nations Commission on International Trade Law and United Nations Convention on Contracts for the International Sale of Goods as to the interpretation or enforcement of the Agreement and waives and "opts out" of the Uniform Computer Information Transactions Act (UCITA), or such other similar laws as may have been adopted.

15.2 The invalidity or illegality of any provision in this Agreement will not affect the validity of any other provision. All unaffected provisions remain in full force and effect.

15.3 Customer may not assign this Agreement without Kronos' prior written consent.

15.4 If there is some unforeseen event reasonably beyond the control of each of the Parties, such as acts of war, terrorism, or uprising, or acts of nature like earthquakes or floods, or civil unrest like embargoes, riots, sabotage or labor shortages, or changes in laws or regulations, or the failure of the internet or communications via common networks, or a power failure, or a delay in transportation, (collectively "Force Majeure"), each Party will be excused from performance of its obligations under this Agreement for the duration of the Force Majeure affecting such Party. The affected Party will use reasonable efforts to mitigate the impact of the Force Majeure on the other Party. Kronos is still obligated to provide the disaster recovery portion of the Service if Kronos' performance of those disaster recovery services is not also prevented by the Force Majeure.

15.5 When either Party needs to provide official notification under this Agreement, those notices will be in writing and considered delivered upon actual receipt to the addresses stated on the relevant Order Form or as otherwise communicated in writing to each other. Each Party agrees that an e-signature (or a facsimile signature by the authorized representative) is evidence of acceptance of a valid and enforceable agreement.

15.6 No third party beneficiaries exist under this Agreement.

15.7 This Agreement (and any information in any referenced Exhibit or at any referenced URL or specifically incorporated by reference) along with the corresponding Order Form constitutes the entire agreement between the Parties pertaining to each Order Form. This Agreement supersedes all prior and contemporaneous representations, negotiations or communications between the Parties relating to its subject matter. This Agreement may only be amended in writing signed by each of the Parties. If Customer uses its own purchase order as an Order Form, no pre-printed terms of that purchase order shall apply to the items ordered, and any reference to a Kronos quote number or order number shall be deemed to incorporate that Kronos quote or order form into Customer's purchase order.

15.8 INSURANCE.
Kronos shall provide the following minimum insurance coverages (in addition to Kronos' insurance coverage requirements set forth in the Information Privacy and Security Agreement attached hereto as Attachment H):

a. Worker's compensation and employer's liability insurance as required by the State of Washington;
b. General commercial liability 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 Kronos' field of expertise, in the amount not less than two million dollars ($2,000,000) against claims arising out of work provided for in this Agreement.
d. 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 Services; and (iv) loss of data or denial of service incidents.

The amounts listed above are the minimum deemed necessary by the Customer to protect the Customer's interests in this matter. The Customer has made no recommendation to Kronos as to the insurance necessary to protect Kronos' interests and any decision by Kronos to carry or not carry insurance amounts in excess of the above is solely that of Kronos. Kronos' maintenance of insurance as required by this Section 15.8 shall not be construed to limit the liability of Kronos to the coverage provided by such insurance, or otherwise limit the City's recourse to any remedy available at law or equity.

All insurance shall be obtained from an insurance company authorized to do business in the State of Washington. Excepting the professional liability insurance, the Customer will be named on all insurance as an additional insured. Kronos shall submit a certificate of insurance to the Customer evidencing the

coverages specified above, together with an additional insured endorsement or a blanket additional insured endorsement, within fifteen (15) days of the execution of this Agreement. Kronos' insurance shall be primary and non-contributing as to the Customer. The certificates of insurance shall cover the work specified in or performed under this Agreement. Kronos shall notify the Customer in the event of cancellation, reduction or substantial modification of the foregoing policies with a thirty (30) days prior written notice to the Customer. Receipt by Customer of any certificate showing less coverage than required is not a waiver of Kronos' obligations to fulfill the requirements of this Agreement.

Attachment A-2: Professional and Educational Services Policies:

Attachment A-3: Service Level Agreement:

The following are the policies under which Kronos will operate during the course of a customer engagement:

1. Kronos will provide the Customer with a Statement of Work (also known as the SOW) that outlines the project deliverables and provides an estimate for the project scope and cost required to complete the engagement, based upon preliminary information provided by the Customer. This Statement of Work is an estimate; the Collaborate Phase of the engagement will be used to determine whether modifications to the project scope or project budget are required.
2. The Statement of Work is valid for one year from the date of signature.
3. Any changes to the project scope and/or project duration will be reflected through the generation of a Kronos Change Order, which is initiated by the Kronos Project Manager and approved and signed by the Customer.
    a. These changes could be due to an increase or change in project scope or deliverables, insufficient customer resources or time commitment, changes to customer project schedule, or technical limitations.
4. Unless otherwise addressed within these policies, the hourly rate(s) quoted within a Change Order for work to be performed within normal business hours will be consistent with that contained within the original Statement of Work. In instances where specialized resources are requested, but not contained within the original Statement of Work, the quoted rate will be established as Kronos' current rate for such requested services.
5. Kronos personnel working at the Customer site shall have access to necessary infrastructure (servers, network, etc.).
6. In instances where Kronos personnel are working remotely access will be granted through the use of industry standard tools (VPN, DTS, GoToMyPC, PCAnywhere, etc.).
7. Customer agrees to not hire any Kronos employee who has performed services under the Agreement for a period of one-year after the completion of such services
8. If not hosted by Kronos Cloud Services, all required system administration, maintenance, backups, tuning, etc., is the responsibility of the Customer
9. Customer Data: To perform the implementation and to provide support after completion, Kronos may need to access and retain information regarding your employees and business organization. Kronos will take all reasonable steps to limit and safeguard the security of this information.
10. Scheduled Work Policies:
    a. Professional Services
        i. Professional Services work will be conducted during normal business hours, 8:00AM – 5:00PM, Monday through Friday, Pacific Standard Time.
        ii. All Professional Services work scheduled to start outside of normal business hours will be billed in full at a premium rate described below. For work to be performed after hours, on holidays, or on weekends, an approved Change Order will be required prior to scheduling (see Change Order Process below). Customers will be charged as follows:
            1. All Professional Services will be scheduled and billed in 4 hour increments with a minimum charge of 4 hours.
                a. After Hours

i. All scheduled work will be billed at 1.5 times the contract rate by role
ii. After Hours is considered 5:00PM-8:00AM, Monday through Friday

b. Weekends
i. All scheduled work will be billed at 2.0 times the contract rate by role
ii. Weekends are considered 5:00PM Friday through 8:00AM Monday

c. Holiday
i. All scheduled work will be billed at 2.0 times the contract rate by role
ii. Holidays are any Kronos recognized Holidays, which include: New Year's Day, President's Day, Memorial Day, Independence Day, Thanksgiving Day, the day after Thanksgiving, Christmas Day.

b. Education Services
i. All training course delivery scheduled to start outside of normal business hours will be billed in full at a premium rate described below. Customers will be charged as follows:

1. After Hours
a. There will be a 1.5 times premium per student for public courses or per class for private day rates
b. After Hours is considered 5:00PM-8:00AM, Monday through Friday

2. Weekends
a. There will be a 2.0 times premium per student for public courses or per class for private day rates
b. Weekends are considered 5:00PM Friday through 8:00AM Monday

3. Holidays
a. There will be a 2.0 times premium per student for public courses or per class for private day rates
b. Holidays are any Kronos recognized Holidays, which include: New Year's Day, President's Day, Memorial Day, Independence Day, Thanksgiving Day, the day after Thanksgiving, Christmas Day.

11. Travel Policies
a. Customer is responsible for airfare, lodging and related travel expenses for onsite consultants.
b. Customer is responsible for travel costs for employees attending training at a Kronos location.
c. Customer is responsible for travel and related costs for a Kronos trainer providing instruction at the Customer location.
d. If a Kronos employee is required on-site per the customer request, a minimum of4 hours will be billed per day.

12. Cancellation Policies: Kronos requires notification for the cancellation or rescheduling of Kronos personnel as well as the cancellation of Instructor led classes. Customer will be charged for failure to meet the following notification requirements:
a. Professional Services:

i. 2 business days prior to scheduled work – 50% of planned charges are invoiced for schedule work
ii. 1 business day prior to scheduled work – 100% of planned charges are invoiced for scheduled work
iii. Business days are: Monday, Tuesday, Wednesday, Thursday, and Friday, excluding Holidays

b. Education Services:

i. For any PUBLIC course held in the traditional classroom or in the virtual classroom, attendees must cancel at least five business days before the class start date to avoid cancellation fees (equal to the cost of the course). Student substitutions can be made at any time as long as prerequisites have been met.
ii. For any PRIVATE course held at a customer site, in the traditional classroom, or in the virtual classroom: attendees must cancel at least ten business days before the class start date to avoid cancellation fees (equal to the cost of the course). Student substitutions can be made at any time as long as prerequisites have been met.
iii. Kronos reserves the right to cancel classes up to five business days before the scheduled start date for public courses held in a Kronos Traditional Classroom (KTC) and up to two business days before the scheduled start date for public courses held in a Kronos Virtual Classroom (KVC) due to lack of enrollment or any other unforeseen circumstances.
iv. Educational Services purchases are valid for one (1) year from the date of signature. Educational Service purchased but not used within this one year period will expire.

c. Cancellation Policy Example:

i. Work is schedule for Wednesday, 1p-5p (4 hours)
ii. If customer cancels on:
    1. Friday – no penalty
    2. Monday – 50% of planned charges are invoiced (2 hours)
    3. Tuesday – 100% of planned charged are invoiced (4 hours)
iii. Cancellation Policy Example with a Holiday:
    i. Work is schedule for Wednesday, 1p-5p (4 hours)
    ii. If customer cancels on:
        1. Thursday – no penalty
        2. Friday – 50% of planned charges are invoiced (2 hours)
        3. Monday – holiday, doesn't count as "business day
        4. Tuesday – 100% of planned charged are invoiced (4 hours)

13. Additional Education Services Policies

a. All Instructor-led Educational Services classes will be held at a Kronos facility, or via the Kronos Virtual Classroom (if offered in that modality), unless Customer has purchased onsite location training.

WORKFORCE DIMENSIONS SERVICE LEVEL AGREEMENT (WFD SLA)

Service Level Agreement: Kronos offers the Service Level Agreement and associated SLA Credits as described in this WFD SLA. This WFD SLA does not apply to the Boomi development environment described in the Exhibit - AtomSphere Service and Boomi Software.

Availability: The production environment of the Service will maintain **99.75% Availability**. SLA Credits become available starting the month after Customer's written "go live" confirmation is provided to Kronos.

SLA Credits: If, due to an Outage, the Service does not maintain 99.75% Availability, Customer is entitled to a credit to Customer's monthly invoice for the affected month, such credit to be equivalent to 3% of Customer's monthly PEPM Fees for every 1% of Availability below 99.75%, but in no event to exceed 100% of Customer's monthly PEPM Fees.

"Outage" means the accumulated time, measured in minutes, during which Customer is unable to access the production environment for the Service for reasons other than an Excluded Event.

"Excluded Event" means any event that causes unavailability to the Service due to (a) the acts or omissions of Customer, its employees, customers, contractors or agents; (b) the failure or malfunction of equipment, applications or systems not owned or controlled by Kronos or its third party suppliers providing the Service; (c) failures or malfunctions resulting from circuits provided by Customer; (d) any inconsistencies or changes in Customer's source environment, including either intentional or accidental connections or disconnections to the environment; (e) Customer Data; (f) Force Majeure events; (g) expected downtime during the Maintenance Periods described below; (h) any suspension of the Service in accordance with the terms of the Agreement; (i) the unavailability of required Customer personnel, including as a result of failure to provide Kronos with accurate, current contact information; or (j) using an Application in a manner inconsistent with the Documentation for such Application.

"Maintenance Period" means scheduled maintenance periods established by Kronos to maintain and update the Services, when downtime may be necessary. Customer chooses maintenance window based on location of data center selected on Order Form.

The Maintenance Period is used for purposes of the Service Credit Calculation; Kronos continuously supports the production environment on a 24x7 basis to reduce disruptions.

The current weekly Maintenance Period for each of the data center locations are:

- US/Canada Eastern Time from Saturday, 12:00 AM - 4:00 AM
- Australian Eastern Time from Saturday, 12:00 AM - 4:00 AM or

- Central European Time Saturday, 2:00 AM - 6:00 AM.

Effective 11 July 2019, the weekly Maintenance Period will change to:

- US/Canada Eastern Time from Thursday, 12:00 AM - 4:00 AM
- Australian Eastern Time from Thursday, 12:00 AM - 4:00 AM or
- Central European Time Thursday, 2:00 AM - 6:00 AM.

Service Credit Calculation: An Outage will be deemed to commence when the Service is unavailable to Customer and ends when Kronos has restored availability to the Service.

Availability Percentage: (Monthly Minutes (MM) minus Total Minutes Not Available (TM)) multiplied by 100 and then divided by Monthly Minutes (MM), but not including Excluded Events.

"Monthly Minutes (MM)" means the total time, measured in minutes, of a calendar month commencing at 12:00 am of the first day of such calendar month and ending at 11:59 pm of the last day of such calendar month.

"Total Minutes Not Available (TM)" means the total number of minutes during the calendar month that the Service is unavailable as the result of an Outage.

Reporting and Claims Process

Kronos will provide Customer with Availability metrics on a monthly basis for each prior calendar month. Customer must request the applicable SLA Credits by written notice to Kronos within sixty (60) days of receipt of the metrics. Customer waives any right to SLA Credits not requested within this time period. All performance calculations and applicable SLA Credits are based on Kronos' records and data unless Customer can provide Kronos with clear and convincing evidence to the contrary.

Outages in one production environment may not be added to Outages in any other production environment for purposes of calculating SLA Credits.

Customer acknowledges that Kronos manages its network traffic in part on the basis of Customer's utilization of the Service and that changes in such utilization may impact Kronos' ability to manage network traffic. Therefore, notwithstanding anything else to the contrary, if Customer significantly changes its utilization of the Service than what is contracted with Kronos and such change creates a material and adverse impact on the traffic balance of the Kronos network, as reasonably determined by Kronos, the Parties agree to co-operate, in good faith, to resolve the issue.

Tenants included	One standard production tenant One partial copy non-production tenant limited to 18 months of data
Additional tenants	Additional partial copy tenants available for purchase on an annual basis
Connectivity to	The customer's end users connect to Workforce Dimensions applications via a secure SSL/TLS connection over **service** the internet. Cooperation between Kronos and the customer's IT staff may be required to enable access. Kronos will assist with validating site connectivity but assumes no responsibility for the customer's internet connection or ISP relationships. Kronos-related internet traffic cannot be filtered by proxy or caching devices on the client network. Workforce Dimensions supports vanity URL, utilizing a single domain.
SFTP accounts	The Kronos cloud SFTP service provides a generic endpoint for customers to push and pull files — including people import, payroll, accruals, schedules, punches, drivers, and more — to and from the Kronos cloud in support of Kronos® integrations. The service includes two SFTP managed service accounts that customers may use to automate their integrations with the Kronos cloud. All managed service account logins use public key authentication to secure files in transit. Transfers of files up to 100MB are supported. Customers may also purchase additional managed service accounts. User accounts for individual (named) customer login are not supported by the SFTP service.
MPLS/Site-to-cloud (optional)	Customers choosing to utilize MPLS are required to use connections offered by Google Cloud Interconnect service providers and will pay the service provider directly. Kronos will assist in provisioning of the link.
Server-initiated device (optional)	Supported per Documentation (includes two VPN connections)

Secure file transfer	Integration with Kronos Workforce Dimensions using the Kronos Cloud SFTP service is subject to the following limits: **limits** - 20 active concurrent sessions per SFTP account - File size transferred per SFTP session not to exceed 100MB - Storage quota of 10GB per SFTP account
Key performance indicators (KPIs)	KPIs can be used to monitor and control business targets and thresholds. Many KPIs are delivered to the customer to track common workforce metrics such as overtime and labor costs. The customer has the option to build additional organization-specific KPIs using the KPI Builder. The number of active KPIs used with Workforce Dimensions applications will be limited to 200 per customer. Additional KPIs may be purchased.
Server-initiated device (optional)	Supported per Documentation (includes two VPN connections)

Data refresh	Customer can request that a copy of production tenant be moved to its non-production tenant once per week — up to the limit of data allowable in the non-production tenant.
Kronos application updates	Maintenance updates will be automatically applied as needed. New software releases will be automatically applied according to the release schedule published during the first month of each quarter.
Customer termination	Upon customer termination, Kronos will provide access to the service for an additional 30 days so the **support** customer may extract data.
Security compliance	A SOC 2 Type 1 report will be published during the first quarter after general availability release. A SOC 2 Type 2 report will be published 12 months after general availability release.
Disaster recovery	Recovery time objective: 24 hours Recovery point objective: 4 hours
Encryption	Data encryption in transit and at rest is included.
Third parties	The customer may contract with a third party to configure and/or implement Workforce Dimensions applications. The customer will be responsible for creating users in the system for the third party to access the application and for maintaining the permissions those users have within the

	application. Dedicated service and support accounts can be accessed only by Kronos personnel or contractors employed by Kronos.
Legal Hold	Kronos will comply with applicable laws and regulations when responding to subpoenas and inquiries from government agencies after consultation with customers when applicable and possible. In the event that a customer is subject to a subpoena, litigation discovery request, or government inquiry directed at customer data or documents that are solely within Kronos' control, Kronos will, at the customer's request, make commercially reasonable efforts to provide assistance to the extent that it is technically feasible. The customer will reimburse Kronos for the costs that Kronos incurs to provide such assistance, such as professional services fees, copying, delivery, and other handling expenses. Subject to the above, Kronos will produce the relevant data or documents. Except at its sole discretion or if legally required to do so, Kronos will not entertain requests to store or host legacy or archived customer data or documents for these purposes. Kronos periodically reviews all matters subject to legal hold, including data that is being retained.

Exhibit C: Success Plans

Section 1. Success Plans

1.1 Kronos offers the following Success Plans for Workforce Dimensions:

a. Community Success (included in Customer's PEPM Fee)

b. Guided Success (available for an additional Fee)

c. Signature Success (available for an additional Fee with minimum annual spend in PEPM and Equipment Rental Fees)

1.2 As part of the Community Success Plan, Kronos will provide:

a. Local Time Zone Support: 8am – 8pm Monday to Friday, with two-hour response time to support cases.

b. 24/7 Mission Critical Support: Immediate and on-going support for a critical issue with no available workaround, where the system or a module may be down, experiencing major system degradation, or other related factors.

c. Kronos Community Access: Ability to access how-to articles, discussion boards, and open support cases .

d. Kronos Onboarding Experience: Step-by-step guidance to assist Customer during onboard activities.

e. KnowledgeMap™: On-line education portal providing access to Kronos e-learning resources.

e. KnowledgeMap™ Live may be purchased for an additional Fee.

f. A Technical Account Manager (TAM) may be purchased for an additional Fee: senior Technical Support Engineers or former Kronos Application Consultants with industry-specific Kronos product knowledge.

1.3 As part of the Guided Success Plan, Kronos will provide:

a. All of the services under Community Success, including the option to purchase KnowledgeMap™ Live or a TAM.

b. Proactive Support: Monitoring of your environment and usage with proactive notification and resolution of potential issues.

c. Named Success Manager: Dedicated, industry-specific advisor.

d. Live Check-In Meetings: Regular meetings with your named success manager.

e. Personalized Success Path: Tailored guidance based on your business goals.

f. Success Reporting: Personalized reporting providing insight into your key performance indicators on an annual basis (i.e., user adoption, compliance, productivity, efficiency.)

g. Executive Business Review: Strategic review of roadmap, realized value, engagement, relationship, and future direction.

h. Optimization Assessment: Assistance with optimizing the use of Workforce Dimensions based on your current usage patterns.

1.4 As part of the Signature Success Plan, Kronos will provide:

a. All of the services under Guided Success. Additionally, KnowledgeMap™ Live and a TAM are included as part of the Signature Success Plan for no additional Fee.

b. 24/7 Local Time Zone Support with one-hour response time to support cases.

c. Technical Account Manager included at no additional charge.

d. Integration/API Support: Assistance with enhancing and updating existing APIs and integrations.

e. KnowledgeMap™ Live included at no additional charge.

k. Industry Best Practice Audit: Review configuration and use of Workforce Dimensions against industry peers and provide recommendations.

1.5 Each Success Plan provides different services and different service coverage periods, which are described in Attachment C-1.

1.6 The Kronos policies set forth in Attachment C-2 shall apply to all Success Plans.

Attachment C-1: Success Plans:

Attachment C-2: Support Policies:

These items are charged in addition to the normal monthly per employee per month fee (PEPM) as they are incurred. For each miscellaneous item listed below, there is a brief description of how/when that charge could be incurred.

	COMMUNITY SUCCESS (Included)	GUIDED SUCCESS (Fees apply)	SIGNATURE SUCCESS (Fees apply)
SUPPORT SERVICES			
Local Time Zone Support	8 a.m - 8 p.m. M-F Support 2-hour response time to cases		24-hour x 7 Support 1-hour response time to cases
24x7 Mission Critical Support	•	•	•
Proactive Support		•	•
Technical Account Manager	Fees apply	Fees apply	•
Integration/API Support			•
SUCCESS SERVICES			
Kronos Community	•	•	•
Kronos Onboarding Experience			

	•	•	•
KnowledgeMap™	•	•	•
KnowledgeMap™ Live	Fees apply	Fees apply	•
Live Check in Meetings		Quarterly	Monthly
Personalized Success Paths		•	•
Success Reporting		Semi-Annually	Quarterly
Executive Business Review		Annually	Quarterly
New Feature Review and Activation		•	•
Optimization Assessment		Semi-Annually	Quarterly
Industry Best Practice Audit			Quarterly

Kronos provides support services for all customer environments (Production and User Acceptance Testing (UAT)) running the Workforce Dimensions Applications. Upgrades to these environments are included in all Success plans. Configuration of new features may be subject to additional cost depending on complexity.

Support Exclusions

Support services do not include service to the Applications resulting from, or associated with:

1. Failure to use the Applications in accordance with Kronos' published specifications; or
2. Customer's end user computer or operating system malfunctions, including browser and internet connection; or
3. Services required for application programs or conversions from products or software not supplied by Kronos.

Service Coverage Period

Kronos provides support for the Workforce Dimensions Infrastructure 24 hours a day, seven days a week, 365 days a year.

Support coverage hours for the Application for use, usability and “how to” questions depend on the Workforce Dimensions Success Plan purchased with the Service.

Local Time Zone Support	**8:00 AM – 8:00 PM Monday to Friday*** 2 hour response to support cases * Excluding Kronos holidays	**24 Hour x 7 support** 1 hour response to support cases

Priority Based Support

Kronos provides support on a "priority" basis. As such, customers with the most critical request(s) will be serviced first. Kronos Global Support has set up the following guidelines to assess the priority of each service request:

High Priority: A critical customer issue with no available workaround where the Applications cannot be accessed, or where the Applications are experiencing major

system degradation, and any other related factors resulting in the customer not being able to process their payroll, such as:

- Cloud outage
- Unable to sign-off Time Cards
- Totals are not accurate
- Unable to collect punches from terminals
- Unable to access a critical function within the Applications such as scheduling

Medium Priority: A serious customer issue which impacts ability to utilize the application effectively such as:

- Intermittent or inconsistent functionality results or data accuracy - accrual balances not matching pay codes but balances are accurate
- Data display inaccuracies or inconsistencies across multiple tasks
- Application performance is inconsistent or fluctuates

Low Priority: Non-critical problem generally entailing use and usability issues or "how to" questions such as:

- How do I set up a holiday pay rule?
- How do I run a report?

Response Time

Response time shall mean the number of hours from the time the case priority is set by the Kronos Support Center until a Kronos technical representative contacts the customer to begin service. Kronos utilizes a priority based support focus. Customers with the most critical request will be serviced in accordance with the following guidelines:

Priority			
High	2 hours	2 hours	1 hours
Medium	4 hours	4 hours	4 hours
Low	8 hours	8 hours	8 hours

Critical Outages

Kronos will provide continuous effort on all high priority events through either bug identification, the development of a workaround, or problem resolution. If this effort goes beyond normal business hours, the case may be passed to the after-hours team. On-

going continuous effort may also be dependent on the customer's ability to provide a resource to work with Kronos during this period.

Technical Escalation

Kronos' case resolution process is a team based approach structured around specific features within the Application suite and staffed by Kronos Support Engineers covering the full spectrum of skill sets and technical expertise. The teams are empowered to dynamically apply the appropriate resources to a case based on severity and complexity to ensure the fastest resolution time possible.

The teams are also integrated with the Development Engineering and Cloud Operations staff and engage their assistance and technical guidance when necessary and/or directly escalate depending on case severity and time to resolve considerations.

For situations that contain multiple cases, an Account Manager may be assigned to act as a single point of contact and communication regarding case resolution status, action plan development, resource integration and implementation co-ordination. The Account Manager remains engaged until the situation has been successfully remediated.

Management Escalation

Customers may, at any time, ask to speak to a Kronos manager if they experience dissatisfaction with the level of service received with respect to a specific case or service in general. To contact a Kronos Global Support manager, please telephone your Kronos Support Services center and ask to speak to a manager. Phone numbers are listed on the Kronos Community at https://community.kronos.com/s/article/ka361000000ACDuAAO/KB13193.

Remote Support

A web-based screen-sharing application that enables Kronos to support you by empowering our support representatives to remotely view your computer. By connecting through the Internet or via intranets and extranets, support representatives will work in real time with your users and quickly escalate to desktop sharing, which features mutual mouse and keyboard control and whiteboard capability.

Kronos Community

The Community helps you make the most of your Kronos solution by putting tools and resources at your fingertips in a collaborative, intuitive online space — a space that makes opening a case, accessing support, and viewing all your account information easier than ever. Streamlined and searchable, the information you need is just a click away.

Exhibit D: Acceptable Use Policy

This Acceptable Use Policy (this **"Policy"**) describes prohibited uses of the Service. The examples described in this Policy are not exhaustive. Kronos may modify this Policy at any time upon written notice to Customer of a revised version. By using the Service, Customer agrees to the latest version of this Policy. If Customer violates the Policy or authorizes or helps others to do so, Kronos may suspend use of the Service until the violation is corrected, or terminate the Agreement for cause in accordance with the terms of the Agreement.

No Illegal, Harmful, or Offensive Use or Content

Customer may not use, or encourage, promote, facilitate or instruct others to use, the Service for any illegal, harmful or offensive use, or to transmit, store, display, distribute or otherwise make available content that is illegal, harmful, or offensive. Prohibited activities or content include:

- **Illegal Activities.** Any illegal activities, including advertising, transmitting, or otherwise making available gambling sites or services or disseminating, promoting or facilitating child pornography.
- **Harmful or Fraudulent Activities.** Activities that may be harmful to others, Kronos' operations or reputation, including offering or disseminating fraudulent goods, services, schemes, or promotions (e.g., make-money-fast schemes, ponzi and pyramid schemes, phishing, or pharming), or engaging in other deceptive practices.
- **Infringing Content.** Content that infringes or misappropriates the intellectual property or proprietary rights of others.
- **Offensive Content.** Content that is defamatory, obscene, abusive, invasive of privacy, or otherwise objectionable, including content that constitutes child pornography, relates to bestiality, or depicts non-consensual sex acts.
- **Harmful Content**. Content or other computer technology that may damage, interfere with, surreptitiously intercept, or expropriate any system, program, or data, including viruses, Trojan horses, worms, time bombs, or cancelbots.

No Security Violations

Customer may not use the Service to violate the security or integrity of any network, computer or communications system, software application, or network or computing device (each, a "System"). Prohibited activities include:

- **Unauthorized Access.** Accessing or using any System without permission, including attempting to probe, scan, or test the vulnerability of a System or to breach any security or authentication measures used by a System. Customer will not perform any security integrity review, penetration test, load test, denial of service simulation or vulnerability scan on any System.

- **Interception.** Monitoring of data or traffic on a System without permission.
- **Falsification of Origin.** Forging TCP-IP packet headers, e-mail headers, or any part of a message describing its origin or route. This prohibition does not include the use of aliases or anonymous remailers.
- **No Use of Robots.** Customer will not use any tool designed to automatically emulate the actions of a human user (e.g., robots)

No Network Abuse

Customer may not make network connections to any users, hosts, or networks unless Customer has permission to communicate with them. Prohibited activities include:

- **Monitoring or Crawling.** Monitoring or crawling of a System that impairs or disrupts the System being monitored or crawled.
- **Denial of Service (DoS).** Inundating a target with communications requests so the target either cannot respond to legitimate traffic or responds so slowly that it becomes ineffective.
- **Intentional Interference.** Interfering with the proper functioning of any System, including any deliberate attempt to overload a system by mail bombing, news bombing, broadcast attacks, or flooding techniques.
- **Operation of Certain Network Services.** Operating network services like open proxies, open mail relays, or open recursive domain name servers.
- **Avoiding System Restrictions.** Using manual or electronic means to avoid any use limitations placed on a System, such as access and storage restrictions.

No E-Mail or Other Message Abuse

Customer will not use the Service to distribute, publish, send, or facilitate the sending of unsolicited mass e-mail or other messages, promotions, advertising, or solicitations (like "spam"), including commercial advertising and informational announcements. Customer will not alter or obscure mail headers or assume a sender's identity without the sender's explicit permission. Customer will not collect replies to messages sent from another internet service provider if those messages violate this Policy or the acceptable use policy of that provider.

Monitoring and Enforcement

Kronos reserves the right, but does not assume the obligation, to investigate any violation of this Policy or misuse of the Service. Kronos may:

- investigate violations of this Policy or misuse of the Service; or
- remove, disable access to, or modify any content or resource that violates this Policy.

Kronos may report any activity that it suspects violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. Kronos' reporting may include disclosing appropriate customer information. Kronos also may cooperate with appropriate law enforcement agencies, regulators, or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this Policy.

Reporting of Violations of this Policy

If Customer becomes aware of any violation of this Policy, Customer will immediately notify Kronos and provide Kronos with assistance, as requested, to stop or remedy the violation

Exhibit E: AtomSphere Service and Boomi Software

As part of the Service, Customer has the right to access and use the Boomi AtomSphere Service and a non-exclusive, non-transferable and non-sublicensable license to use the associated Boomi Software as part of the Boomi AtomSphere Service. Customer may use the Boomi AtomSphere Service and the Boomi Software only to create integrations to and from the Service.

There are two (2) cloud environments associated with Customer use of the Boomi AtomSphere Service and the Boomi Software:

a. Run-Time environment: A run time environment in the Kronos Cloud where the integration created by with the Boomi AtomSphere Service runs. This environment is described in Exhibit B.
b. Development environment: A development environment in the Boomi Cloud where the design and development tools exist to build the integrations. This environment is referred to as a Hosted Environment in Attachment E-1.

The Boomi AtomSphere Service is subject to the additional terms and conditions set forth below. These additional terms and conditions apply to all integrations to and from the Service using the Boomi AtomSphere Service, whether done by Customer or by Kronos. Except as provided in these additional terms and conditions, all terms and conditions of this Agreement related to the Service apply to the Boomi AtomSphere Service. If this Agreement terminates, Customer's rights to access the Boomi AtomSphere Service and the Boomi Software also terminates.

Attachment E-1: Boomi Flow Down Provisions:

Exhibit F: Definitions

"Acceptable Use Policy" and **"AUP"** are interchangeable terms referring to the Kronos policy describing prohibited uses of the Service as further described in Exhibit D.

"Add In(s)" mean the Kronos developed applets for Workforce Dimensions that enable limited functionality through the application programming interfaces ("APIs") of Workforce Dimensions and the associated applications of certain third-party technology providers as further described in Exhibit G.

"Aggregated Data" is any statistical data that is derived from the operation of the Service, including without limitation, for analysis of the Service, Configurations or Customer Data, and is created by Kronos in response to specified queries for a set point in time; including without limitation aggregation, metrics, trend data, correlations, benchmarking, determining best practices, the number and types of transactions, configurations, records, reports processed in the Service, and the performance results for the Service Agreement.

"Applicable Law(s)" means any applicable provisions of all laws, codes, legislative acts, regulations, ordinances, rules, rules of court, and orders which govern the Party's respective business.

"Authorized User" means any individual or entity that directly (or through another Authorized User) accesses or uses the Service with any login credentials or passwords Customer uses to access the Service.

"Application(s)" means those Kronos Workforce Dimensions software application programs set forth on an Order Form which are made accessible for Customer to use under the terms of this Agreement.

"Boomi AtomSphere Service" means the third-party service for the creation of integrations by Customer as further described in Exhibit E, which the Customer and Customer's Authorized Users have the right to access through the Service.

"Boomi Software" means the third-party proprietary software associated with the Boomi AtomSphere Service as further described in Exhibit E.

"Claim(s)" means any and all notices, charges, claims, proceedings, actions, causes of action and suits, brought by a third party.

"Confidential Information" is any non-public information relating to each of Customer's and Kronos' businesses and those of Kronos' Technology suppliers that is disclosed pursuant to this Agreement and which reasonably should have been understood by the recipient of such information to be confidential because of (i) legends or other markings, (ii) the circumstances of the disclosure, or (iii) the nature of the information itself. Information will not be considered "Confidential Information" if the information was (i) in the public domain without any breach of this Agreement; (ii) disclosed to the Receiving Party on a non-confidential basis from a source which is lawfully in possession of such Confidential Information and, to the knowledge of the Receiving Party, is not prohibited from disclosing such Confidential Information to Receiving Party; or (iii) released in writing from confidential treatment by Delivering Party; or (iv) required to be disclosed pursuant to a subpoena, order, civil investigative demand or similar process with which the Receiving Party is legally obligated to comply, and of which the Receiving Party notifies Delivering Party.

"Configuration(s)" means the Customer specific settings of the parameters within the Applications(s), including pay and work rules, security settings such as log-in credentials, passwords, and private keys used to access the Service.

"Controls" means the administrative, physical, and technical safeguards for the protection of the security, confidentiality and integrity of Customer Data, designed and implemented by Kronos to secure Customer Data against accidental or unlawful loss, access or disclosure consistent with the AICPA Trust Principles Criteria for security, availability, confidentiality and processing integrity (SOC 2).

"Customer Data" means all content Customer, or its Authorized Users, posts or otherwise inputs into the Service, including but not limited to information, data (such as payroll data, vacation time, hours worked or other data elements associated with an Authorized User), text, multimedia images (e.g. graphics, audio and video files), or compilations.

"Customer Indemnified Party(ies)" means Customer and Customer's respective directors, officers, and employees.

"Data Protection Law(s)" means all international, federal, state, and local laws, rules, regulations, directives and published governmental or regulatory decisions that specify data privacy, data protection or data security obligations, and which, in each case, have the force of law applicable to a Party's collection, use, processing, storage, or disclosure of Personally Identifiable Information.

"Documentation" means the published specifications for the applicable Applications and Equipment, such as user manuals and administrator guides.

"Educational Services" means (i) KnowledgeMap Learning Portal; (ii) KnowledgeMap Live; and (iii) ala carte educational consulting services.

"Equipment" means Kronos equipment such as time clocks, devices, or other equipment set forth on an Order Form.

"Equipment Support Services" means the maintenance and support services related to Kronos' support of Equipment as further described in Attachment A-1.

"Feedback" means suggestions, ideas, comments, know how, techniques or other information provided to Kronos for enhancements or improvements, new features or functionality or other feedback with respect to the Service.

"Fees" means the charges to be paid by Customer for a particular item.

"Implementation Services" means those professional services provided by Kronos to set up the cloud environment and to setup the Configurations within the Applications, as set forth in an SOW.

"KnowledgeMap™" means the online educational portal providing access to learning resources.

"KnowledgeMap™ Live" means the subscription service providing instructor led training by user role on a rotating course schedule.

"Kronos Indemnified Party(ies)" means Kronos and its third-party Technology suppliers and each of their respective directors, officers, employees, agents and independent contractors.

"Order Form" means an order form mutually agreed upon by Kronos and Customer setting forth, among other things, the items ordered by Customer and to be provided by Kronos and the Fees to be paid by Customer.

"Participating Entity(ies)" means those Kronos or Customer entities that (i) directly or indirectly control, are controlled by, or are under common control with Kronos or Customer, respectively and (ii) sign an Order Form for the Service. "Control" (in this context) means the possession, directly or indirectly, of the power to direct or cause the direction of the management and operating policies of the entity in respect of which the determination is being made through the ownership of the majority of its voting or equity securities, contract, voting trust or otherwise.

"Party(ies)" means Kronos or Customer, or both of them, as the context dictates.

"PEPM" means the per employee per month fee for a Customer's Authorized Users access to the Service.

"Personally Identifiable Information" means information concerning individually identifiable employees of Customer that is protected against disclosure under Applicable Data Protection Law.

"Professional Services" means the professional, consulting, or training services provided by Kronos pursuant to an Order Form and which are not described in a Statement of Work.

"Seasonal Licenses" are limited use licenses that have the following attributes: (i) valid only for the four (4) consecutive months during the annual period identified on the Order Form; (ii) valid from the first day of the month in which they commence until the end on the last day of the month in which they expire; and (iii) will be effective automatically each year during the Term, subject to termination and non-renewal as provided in the Agreement.

"Service" means the Kronos supply of the commercially available version of the Workforce Dimensions SaaS Applications in Kronos' hosted environment and the services described in the Agreement related thereto.

"Statement of Work" and **"SOW"** are interchangeable terms referring to a written description of the Implementation Services.

"Success Plan(s)" means the services provided by Kronos to support and maintain the Service as described in Exhibit C.

"Taxes" means all applicable taxes relating to the goods and services provided by Kronos hereunder, including all duties and country, federal, state, provincial or local taxes (including GST or VAT if applicable) but excluding taxes on Kronos' income or business privilege.

"Technology" means the intellectual property of Kronos within the Service, including but not limited to the Applications.

"Term" means the Initial Term and any Renewal Terms.

Exhibit G: Workforce Dimensions™ Add-Ins

This Exhibit governs the Add-In(s) to be provided by Kronos to Customer, if specified on an Order Form. Capitalized terms not otherwise defined herein shall have the meanings prescribed to them in the Agreement. In the event of a conflict or inconsistency between the Agreement and this Exhibit, this Exhibit shall control.

Customer agrees that the Add-In(s) may only be used solely in connection with Workforce Dimensions™ for Customer's own internal purposes. The Add-Ins are not installed in the Kronos hosting environment in which Workforce Dimensions resides. The Add-Ins may only be installed and operated in a data center or other cloud environment managed by or on behalf of Customer. Customer is solely responsible to have all applicable rights, licenses and necessary infrastructure and support to use the third-party applications with which the Add-In(s) function, including security of the environment in which the Add-In(s) are installed.

The Service Level Agreement and associated SLAs (Attachment A-3) and the Workforce Dimensions Cloud Guidelines (Exhibit B) in the Agreement do not apply to the Add-In(s) because the Add-In does not reside in Kronos' hosting environment.

Implementation. Configuration and deployment of the Add-In(s) may be performed by Customer in accordance with Kronos written instructions and guidelines. Alternatively, Customer may engage Kronos or a third party to perform implementation or professional services as described in the Agreement.

Warranty Disclaimer. Kronos does not warrant that the Add-In(s) will be free from errors or service interruption. Kronos disclaims errors and liability with respect to the third-party applications or APIs with which the Add-In(s) function. Customer is solely responsible to manage its accounts or systems that may access the Add-In(s).

Exhibit H
INFORMATION PRIVACY AND SECURITY AGREEMENT

This Information Privacy and Security Agreement ("IPSA") is entered into by and between the City of Redmond ("City") and Kronos Incorporated ("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 owned and controlled by the City that requires a unique sign-on identification and password, 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, which will be provided by the City to the Contractor's personnel prior to granting credential to access the City owned software system.

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 is satisfied 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 applicable data protection laws and regulations ensuring that the subcontractor has adequate technical and organizational measures in place to protect 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 applicable laws and regulations and with a degree of skill, care, prudence, foresight and practice which would ordinarily be expected of a skilled, experienced and

leading supplier of services of the same or a similar nature to the Services.

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.

   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. Unless Kronos Global Support is requested and consented to by the City 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. 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, improvements to the service, 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 safeguard electronic City Data with encryption controls over such City Data both stored and in transit. 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 a copy of the results of the annual AICPA SSAE 18 SOC 1 and 2 Type II audit reports completed by an independent, 3rd party, tier 1, auditor.

k. 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. For the avoidance of doubt a "potentially significant risk exposure to City Data" shall be defined as an unremediated qualification or exception identified by the 3rd party auditor's report that has the potential to materially and adversely affect the security, confidentiality or availability of City's data.

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 and RCW 42.56.590. Contractor shall report, either orally or in writing, to City any Data Breach involving City Data including any confirmation 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 without undue delay 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.

b. Upon a Data Breach, Contractor is not permitted to notify affected individuals without the express written consent of City, unless required to do so by law. 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 unless such notification is necessary to investigate or remediate the data breach. Contractor is permitted to hire outside contractors to assist in breach investigation and remediation.

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. **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 that are owned and operated by the City.

11. **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. The City will provide a contact person or persons with valid contact information at the time of customer onboarding for notification of a data breach and will be responsible for updating this information as necessary to ensure its accuracy.

    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.