City of Tukwila

Thomas McLeod, Mayor

INFORMATIONAL MEMORANDUM

TO: **Finance & Governance Committee**

FROM: **Nora Gierloff, Community Development Director, Aaron BeMiller, Finance Director, Joel Bush, Chief Technology Officer**

CC: **Mayor Thomas McLeod**

DATE: **April 22, 2025**

SUBJECT: **Contracts for Permitting, Tax, Budget & Transparency Technology Solutions**

ISSUE
The Department of Community Development (DCD), Finance Department (FN), and Technology & Innovation Services (TIS) have partnered in researching and evaluating technology solutions to resolve issues and/or improve processes aimed at enhanced efficiency, transparency, and public access to information.

BACKGROUND
In 2022 the City implemented Central Square Finance Enterprise (FE) as its Enterprise Resource Planning (ERP) software to manage day-to-day operations. The ERP provides a centralized system that serves as the City's accounting system of record and allows all city departments and cross-functional teams to access the system for their individual needs.

Earlier this year, the City began a "gap analysis" of our current ERP comprised by a cross-section of city employees. The gap analysis provides a comparison of the current performance of the ERP with desired or expected performance and looks for reasons preventing meeting the desired system performance. As part of the City's on-going evaluation of FE and its long-term viability as the City's ERP solution, three technology solutions are being requested as an improvement to the current system or to fill a need not offered in the current ERP.

Staff has explored options for transitioning from our current permit tracking platform, *Community Development by Central Square* (formerly called TRAKiT), due to poor performance, lack of support, and excessive staff time spent on workarounds and maintenance. *SmartGov by Granicus,* a modern and comprehensive cloud-based system has been selected as a replacement. SmartGov is currently in use by 51 jurisdictions across Washington State and has a strong track record of improving permitting workflows, enhancing transparency, and expanding public self-service capabilities. This upgrade will improve service delivery and support our broader goals of operational efficiency, accountability, and accessibility.

DISCUSSION
New technology solutions:

SmartGov: Replaces the City's current permitting system with a modern and comprehensive cloud-based system which will improve the user experience for customers, automate many routine tasks, and improve the ability of inspectors to access and update the system in the field. It will also give Tukwila the tools to easily track our compliance with SB 5290, the state mandated permit review process and timeline changes.

OpenGov: Provides solutions not available in the current ERP.

9

- Tax & Revenue: Transitions B&O tax collection from paper to a fully automated online system with compliance tracking. This automation will help build capacity by significantly reducing manual processing and allow our B&O analysts to spend more time in the field performing audits. Additionally, it will provide businesses with a seamless, transparent portal for online tax filing and payments.
- Budget and Planning: Provides the City with a modern budget system to replace the current practice of manually keying budget information into excel spreadsheets. An automated budget system will free up capacity and allow for redeployment of staff to more strategic and value-added work. This solution provides public transparency and community engagement improvements, tracking performance and key performance indicators, as well as dashboards and reports to drive informed policy and business decisions.

FINANCIAL IMPACT

SmartGov: The proposed transition to SmartGov includes an annual software cost of **$38,571** starting in 2025. A **one-time data migration fee of $64,767** will be covered using existing funds from the Technology Fund. For comparison, our current system required an upfront investment of **$312,750** in 2012 and has an ongoing annual operating cost of **$62,805**

OpenGov: Annual software costs in 2025 are $143,500. There is a one-time deployment fee of $116,860. Funding for the tax and revenue component will be paid by B&O collections. Funding for budget, planning, reporting, and transparency component will be paid in 2025 from available fund balance. On-going subscription costs will be allocated as part of the Indirect Cost Allocation Plan. The subscription costs above represent a 25% discount as part of the bundle and will remain in place as part of the on-going subscription costs. However, the discount expires June 2025 if not contracted by then.

RECOMMENDATION

Staff recommends the Committee approve these contracts and forward them to the Consent Agenda for the May 5th, 2025 City Council meeting.

Alternatively, the Committee can forward these contacts to the May 12th, 2025 Committee of the Whole meeting as new business and the May 19th Regular Meeting for adoption.

ATTACHMENTS

- A. Draft SmartGov Contract
- B. Draft OpenGov Contract - *to be provided separately*
- C. OpenGov Executive Summary

City of Tukwila

6200 Southcenter Boulevard, Tukwila WA 98188

Contract Number:_____

CONTRACT FOR SERVICES

This Agreement is entered into by and between the City of Tukwila, Washington, a non-charter optional municipal code city hereinafter referred to as "the City," and _____ hereinafter referred to as "the Contractor," whose principal office is located at _____ . The City and the Contractor are each individually a "Party" and collectively the "Parties."

WHEREAS, the City has determined the need to have certain services performed for its citizens but does not have the manpower or expertise to perform such services; and

WHEREAS, the City desires to have the Contractor perform such services pursuant to certain terms and conditions; now, therefore,

IN CONSIDERATION OF the mutual benefits and conditions hereinafter contained, the parties hereto agree as follows:

1. **Scope and Schedule of Services to be Performed by Contractor.** The Contractor shall perform those services described on **Exhibit A** attached hereto and incorporated herein by this reference as if fully set forth. In performing such services, the Contractor shall at all times comply with all Federal, State, and local statutes, rules and ordinances applicable to the performance of such services and the handling of any funds used in connection therewith. The Contractor shall request and obtain prior written approval from the City if the scope or schedule is to be modified in any way.

2. **Compensation and Method of Payment.** The City shall pay the Contractor for services rendered according to the rate and method set forth on **Exhibit B** attached hereto and incorporated herein by this reference. The total amount to be paid shall not exceed _____ at a rate of_____.

3. **Contractor Budget.** The Contractor shall apply the funds received under this Agreement within the maximum limits set forth in this Agreement. The Contractor shall request prior approval from the City whenever the Contractor desires to amend its budget in any way.

4. **Duration of Agreement.** This Agreement shall be in full force and effect for a period commencing _____, **20__**, and ending _____, **20__**, unless sooner terminated under the provisions hereinafter specified.

5. **Independent Contractor.** The Contractor and the City agree that the Contractor is an independent contractor with respect to the services provided pursuant to this Agreement. Nothing in this Agreement shall be considered to create the relationship of employer and employee between the parties hereto. Neither the Contractor nor any employee of Contractor shall be entitled to any benefits accorded City employees by virtue of the services provided under this Agreement. The City shall not be responsible for withholding or otherwise deducting federal income tax or social security or contributing to the State Industrial Insurance Program, or otherwise assuming the duties of an employer with respect to the Contractor, or any employee of the Contractor.

6. **Indemnification.**

A. <u>Contractor Indemnification</u>. The Contractor shall indemnify, defend and hold harmless the City its officers, officials, employees, volunteers and permitted successors and assigns harmless from any and all claims, injuries, damages, losses or suits including attorney fees (collectively, "Losses"), in connection with any claims, demands, suits or proceedings (collectively, "Claims") made or alleged against the City by a third party arising out of or resulting from the acts, errors or omissions, or the intentional or negligent performance of the Contractor in performance of this Agreement, except for injuries and damages caused by the sole negligence of the City.

B. <u>RCW 4.24.115</u>. However, should a court of competent jurisdiction determine that this Agreement is subject to RCW 4.24.115, then, in the event of liability for damages arising out of bodily injury to persons or damages to property caused by or resulting from the concurrent negligence of the Contractor and the City, its officers, officials, employees, and volunteers, Contractor's liability, including the duty and cost to defend, hereunder shall be only to the extent of Contractor's negligence. It is further specifically and expressly understood that the indemnification provided herein constitutes Contractor's waiver of immunity under Industrial Insurance, Title 51 RCW, solely for the purposes of this indemnification. This waiver has been mutually negotiated by the parties. The provisions of this section shall survive the expiration or termination of this Agreement.

C. <u>Infringement Indemnification</u>. In addition to Contractor's obligations under Section 6.A., the Contractor shall indemnify, defend, and hold harmless the City and its directors, officers, employees, agents and other representatives against any Losses in connection with Claims made or alleged against the City by a third party that the services, software or deliverables infringes a U.S. patent, copyright or other intellectual property rights of any third party. The foregoing indemnification obligation does not apply to any Claims or Losses arising out of or relating to any: (a) access to or use of the software in combination with any hardware, system, software, network or other materials or service not provided or authorized by this Agreement or otherwise in writing by the Contractor; or (b) modification of the software other than: (i) by or on behalf of the Contractor; or (ii) with the Contractor's written approval or in accordance with Contractor's written specifications.

D. <u>Mitigation</u>. If any of the services, software or deliverables are, or in Contractor's opinion are likely to be, claimed to infringe, misappropriate or otherwise violate any third-party intellectual property right, or if the City's or any Authorized User's use of the services, software or deliverables is enjoined or threatened to be enjoined, the Contractor may, at its option and sole cost and expense:

  i. obtain the right for the City to continue to use the Services, Software and Deliverables materially as contemplated by this Agreement;

  ii. modify or replace the services, software and deliverables, in whole or in part, to seek to make the services, software and deliverables (as so modified or replaced) non-infringing, while providing materially equivalent features and functionality; or

  iii. by written notice to the City, terminate this Agreement with respect to all or part of the Services, Software and Deliverables, and require the City to immediately cease any use of the Services, Software and Deliverables or any specified part or feature thereof, provided that if such termination occurs, the Contractor shall refund any prepaid fees to the City and provide transition services free of charge.

12

E.   Limitation of Liability. In no event will either party be liable under or in connection with this agreement or its subject matter under any legal or equitable theory, including breach of contract, tort (including negligence), strict liability and otherwise, for any: (i) loss of revenue or profit; or (ii) consequential, incidental, indirect, exemplary, special, or punitive damages, regardless of whether such persons were advised of the possibility of such losses or damages or such losses or damages were otherwise foreseeable, and notwithstanding the failure of any agreed or other remedy of its essential purpose. In no event shall the aggregate liability of either party arising out of or related to this agreement exceed the greater of two times the fees paid under the agreement or $1,000,000; provided however, the limitation of liability set forth in this section shall not apply to: (i) Contractor's indemnification obligations for infringement claims made or brought against the City by a third party as described herein, or (ii) damages related to claims brought against the City due to Contractor's breach of City's data, including but not limited to damages, penalties or other liabilities arising from government enforcement actions or breach notification requirements. The provisions of this section shall survive the expiration or termination of this agreement.

7.   **Insurance**. Prior to commencing the Services, the Contractor shall procure and maintain at its sole cost and expense at least the following insurance, covering its obligations under this Agreement.

   A.   Insurance Policies.

      i.   *Commercial General Liability:* With coverage of not less than $2,000,000 per occurrence, $2,000,000 general aggregate, and $2,000,000 products-completed operations aggregate limit, which shall cover liability arising from premises, operations, independent contractors, products-completed operations, stop gap liability, personal injury and advertising injury, and liability assumed under an insured contract. Commercial General Liability insurance shall be as least at broad as ISO occurrence form CG 00 01 and shall cover liability arising from premises, operations, independent contractors, products-completed operations, stop gap liability, personal injury and advertising injury, and liability assumed under an insured contract. The Commercial General Liability insurance shall be endorsed to provide a per project general aggregate limit using ISO form CG 25 03 05 09 or an equivalent endorsement. There shall be no exclusion for liability arising from explosion, collapse or underground property damage. The City shall be named as an additional insured under the Contractor's Commercial General Liability insurance policy with respect to the work performed for the City using ISO Additional Insured endorsement CG 20 10 10 01 and Additional Insured-Completed Operations endorsement CG 20 37 10 01 or substitute endorsements providing at least as broad coverage.

      ii.   *Cyber Liability Insurance:* With coverage of not less than $1,000,000 per occurrence and $5,000,000 in the annual aggregate which shall include, but not be limited to, coverage, including defense, for the following losses or services:

         (1) Breach of City's Data, including but not limited to liability arising from theft, dissemination, and/or use of City's confidential and Personal Information as defined by RCW 42.56.590, including but not limited to, any information about an individual maintained by City, including: (a) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (b) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information regardless of how or where the information is stored or transmitted.

13

(2) Network security liability arising from: (a) the unauthorized access to, use of, or tampering with computer systems, by an outside party, including hacker attacks or a virus introduced by a third party; or (b) the inability of an authorized third party to gain access to supplier systems and/or City Data, including denial of service, unless caused by a mechanical or electrical failure; (c) introduction of any unauthorized software computer code or virus causing damage to City Data or any other third party data.

(3) Event management services and first-party loss expenses for a data breach response including crisis management services, credit monitoring for individuals, public relations, legal service advice, notification of affected parties, independent information security forensics firm, and costs to re-secure, re-create and restore data or systems.

iii. Workers' Compensation coverage as required by the Industrial Insurance laws of the State of Washington.

iv. Automobile Liability Insurance of a minimum combined single limit for per occurrence for bodily injury and property damage of $1,000,000 per accident, covering all owned, non-owned, hired and leased vehicles. Coverage shall be written on Insurance Services Office (ISO) form CA 00 01 or a substitute form providing equivalent liability coverage. If necessary, the policy shall be endorsed to provide contractual liability coverage.

v. Professional Liability/Errors and Omissions Insurance (including Technology Errors and Omissions) of at least $1,000,000 per occurrence and $2,000,000 in the annual aggregate.

B. Additional Insurance Requirements.

i. If the Contractor maintains higher insurance limits than the minimums shown above, the City shall be insured for the full available limits of Commercial General and Excess or Umbrella liability maintained by the Contractor, irrespective of whether such limits maintained by the Contractor are greater than those required by this Agreement or whether any certificate of insurance furnished to the City evidences limits of liability lower than those maintained by the Contractor.

ii. The insurance required in Section 7 shall be in a form and on terms and written by insurers with a current A.M. Best rating of not less than A: VII. The Commercial General Liability, Cyber Liability Insurance and Automobile Liability Insurance shall name the City as an additional insured, and shall contain, or be endorsed to contain, that they shall be primary insurance as respect to the City. Any insurance, self-insurance, or self-insured pool coverage maintained by the City shall be excess of the Contractor's insurance and shall not contribute with it.

iii. The Contractor shall provide the City with written notice of any policy cancellation within two business days of the receipt of such notice. Contractor shall obtain replacement insurance policies meeting the requirements of this Section 7.

iv. Failure of the Contractor to maintain the insurance as required shall constitute a material breach of this Agreement, upon which the City may, after giving five business days' notice to the Contractor to correct such breach, immediately terminate this Agreement.

v. The Contractor's maintenance of insurance, its scope of coverage and limits as required herein shall not be construed to limit the liability of the Contractor to the coverage provided by such insurance, or otherwise limit the City's recourse to any remedy available at law or in equity.

14

vi. ***Subcontractor's Insurance.*** The Contractor shall cause each and every subcontractor utilized by the Contractor in connection with the provision of Services ("Subcontractors"), to provide insurance coverage that complies with all applicable requirements of the Contractor-provided insurance as set forth herein, except the Contractor shall have sole responsibility for determining the limits of coverage required to be obtained by Subcontractors. The Contractor shall ensure the City is an additional insured on each and every Subcontractor's Commercial General liability insurance policy, using an endorsement as least as broad as ISO CG 20 10 10 01 for ongoing operations and CG 20 37 10 01 for completed operations.

vii. The Contractor shall furnish the City with original certificates and a copy of the amendatory endorsements, including but not necessarily limited to the additional insured endorsements, evidencing the insurance requirements of the Contractor before commencement of the work. Upon request by the City, the Contractor shall furnish certified copies of all required insurance policies, including endorsements, required in this Agreement and evidence of all subcontractors' coverage.

8. **Record Keeping and Reporting.**

A. Records Maintenance. The Contractor shall maintain accounts and records, including personnel, property, financial and programmatic records which sufficiently and properly reflect all direct and indirect costs of any nature expended and services performed in the performance of this Agreement and other such records as may be deemed necessary by the City to ensure the performance of this Agreement.

B. Retention Period. These records shall be maintained for a period of seven years after termination hereof unless permission to destroy them is granted by the office of the archivist in accordance with RCW Chapter 40.14 and by the City.

C. Public Records Requests. The Contractor acknowledges that the City is a public entity and is subject to the Public Records Act under Chapter 42.56 RCW. To the extent permitted by law, the City shall treat as exempt from treatment as a public record, and shall not disclose in response to a request made pursuant to any applicable public records law, any of the Contractor's Confidential Information. If a request is received for records the Contractor has submitted to the City and has identified as Confidential Information, the City will use its best efforts to provide the Contractor with notice of the request in accordance with RCW 42.56.540 and a reasonable time within which the Contractor may seek an injunction to prohibit the City's disclosure of the requested record. The City shall comply with any injunction or court order requested by the Contractor which prohibits the disclosure of any such Confidential Information; however, in the event a higher court overturns such injunction or court order, the Contractor shall reimburse the City for any fines or penalties imposed for failure to disclose such records. Nothing in this section prohibits the City from complying with RCW 42.56, or any other applicable law or court order requiring the release of public records, and the City shall not be liable to the Contractor for compliance with any law or court order requiring the release of public records.

D. Compelled Disclosures. If either the Party or any of its Representatives is compelled by applicable law to disclose any Confidential Information then, to the extent permitted by law, that Party shall: (a) promptly, and prior to such disclosure, notify the other Party in writing of such requirement so that they can seek a protective order or other remedy or waive its rights under Section 3; and (b) provide reasonable assistance, at the Disclosing Party's cost, to the Disclosing Party in opposing such disclosure or seeking a protective order or other limitations on disclosure. If the Disclosing Party waives compliance or, after providing the notice and assistance required under this section, the Receiving Party remains required by law to disclose

15

any Confidential Information, the Receiving Party shall disclose only that portion of the Confidential Information that the Receiving Party is legally required to disclose. This Section 8.2 shall not apply to Subscriber's response to a request made under the Public Records Act, Chapter 42.56 RCW.

9. **Breach Notification.**

   A. The Contractor shall maintain a data breach plan 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 42.56.590. The Contractor shall report, in writing, to the City any data breach involving data maintained by the Contractor on behalf of the City ("City Data") including any reasonable belief that an unauthorized individual has accessed City Data. The report shall identify the nature of the event, a list of the affected individuals and the types of data, and the mitigation and investigation efforts of the Contractor. The Contractor shall make the report to the City immediately upon discovery of the data breach, but in no event more than five business days after discovery of the data breach. The Contractor shall provide investigation updates to the City.

   B. The Contractor shall promptly reimburse the City in full for all costs incurred by the City in any investigation, remediation or litigation resulting from any data breach. The Contractor's duty to reimburse the City includes but is not limited to, reimbursing to the City its cost incurred in doing the following:

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

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

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

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

10. **City Data.** The Contractor does not claim ownership of, and assumes no responsibility with respect to any City Data defined as information, data, and content, in any form or medium, collected, downloaded, or otherwise received, directly or indirectly from the City, an Authorized Personnel or end-users by or through the Contractor's Services.

11. **Audits and Inspections.** The records and documents with respect to all matters covered by this Agreement shall be subject at all times to inspection, review or audit by law during the performance of this Agreement.

12. **Termination.** This Agreement may at any time be terminated by the City giving to the Contractor 30 days written notice of the City's intention to terminate the same. Failure to provide products on schedule may result in contract termination. If the Contractor's insurance coverage is canceled for any reason, the City shall have the right to terminate this Agreement immediately.

16

13. **Effect of Termination or Expiration.** On the expiration or earlier termination of this Agreement:

   A. Each Party shall continue to hold such Confidential Information in confidence pursuant to Section 8; and

   B. Each Party shall pay to the other all undisputed amounts accrued prior to and through the date of termination of this Agreement; and

   C. The provisions set forth in the following sections, and any other right or obligation of the parties in this Agreement that, by its nature should survive termination or expiration of this Agreement, will survive any expiration or termination of this Agreement.

   D. Within 60 days following such expiration or termination, the Contractor shall deliver to the City, in a format as requested by the City, the then most recent version of City Data maintained by the Contractor, provided that the City has at that time paid all undisputed fees then outstanding and any amounts payable after or as a result of such expiration or termination.

   E. In the event of (i) expiration or earlier termination of this Agreement, or (ii) the City no longer purchasing certain Services from the Contractor, if the City requests assistance in the transfer of City Data to a different vendor's applications ("Deconversion"), the Contractor will provide reasonable assistance. The Parties will negotiate in good faith to establish the relative roles and responsibilities of the Parties in effecting Deconversion, as well as the appropriate date for completion.

14. **Taxes.** The Contractor shall be solely responsible for the payment of any and all applicable taxes related to the Services provided under this Agreement; if such taxes are required to be passed through to the City by law, the same shall be duly itemized on timely billings submitted to the City by the Contractor.

15. **Waiver.** A waiver of any breach by either Party shall not constitute a waiver of any subsequent breach.

16. **Third Party Beneficiaries.** This Agreement is solely for the conveniences of the Parties and there are no third party beneficiaries to this Agreement.

17. **Compliance with Laws.** The Consultant shall comply with all applicable federal, state, and local laws and regulations in performing this Agreement.

18. **Discrimination Prohibited.** The Consultant, with regard to the work performed by it under this Agreement, will not discriminate on the grounds of race, religion, creed, color, national origin, age, veteran status, sex, sexual orientation, gender identity, marital status, political affiliation, the presence of any disability, or any other protected class status under state or federal law, in the selection and retention of employees or procurement of materials or supplies.

19. **Assignment and Subcontract.** The Contractor shall not assign or subcontract any portion of the services contemplated by this Agreement without the written consent of the City.

20. **Entire Agreement; Modification.** This Agreement, together with attachments or addenda, represents the entire and integrated Agreement between the City and the Contractor and supersedes all prior negotiations, representations, or agreements written or oral. No amendment or modification of this Agreement shall be of any force or effect unless it is in writing and signed by the parties.

21. **Severability and Survival.** If any term, condition or provision of this Agreement is declared void or unenforceable or limited in its application or effect, such event shall not affect any other provisions hereof and all other provisions shall remain fully enforceable. The provisions of this Agreement, which by their sense and context are reasonably intended to survive the completion, expiration or cancellation of this Agreement, shall survive termination of this Agreement.

22. **Notices.** Notices to the City of Tukwila shall be sent to the following address:

> City Clerk
> City of Tukwila
> 6200 Southcenter Blvd.
> Tukwila, Washington 98188

> Notices to the Contractor shall be sent to the address provided by the Contractor upon the signature line below.

23. **Applicable Law; Venue; Attorney's Fees.** This Agreement shall be governed by and construed in accordance with the laws of the State of Washington. In the event any suit, arbitration, or other proceeding is instituted to enforce any term of this Agreement, the parties specifically understand and agree that venue shall be properly laid in King County, Washington. The prevailing party in any such action shall be entitled to its attorney's fees and costs of suit.

24. **Force Majeure.** Neither Party shall be responsible for failure to fulfill its obligations hereunder or liable for damages resulting from delay in performance as a result of war, fire, strike, pandemic, riot or insurrection, natural disaster, delay of carriers, governmental order or regulation, complete or partial shutdown of plant, unavailability of equipment, software, or services from suppliers, default of a subcontractor or vendor to the Party if such default arises out of causes beyond the reasonable control of such subcontractor or vendor, the acts or omissions of the other Party, or its officers, directors, employees, agents, contractors, or elected officials, and/or other occurrences beyond the Party's reasonable control ("Excusable Delay" hereunder). In the event of such Excusable Delay, performance shall be extended on a day for day basis or as otherwise reasonably necessary to compensate for such delay.

25. **Counterparts.** This Agreement may be executed in several counterparts, each of which when so executed shall be deemed to be an original, and such counterparts shall constitute one and the same instrument. This Amendment shall be considered properly executed by a Party if executed by that Party and transmitted by facsimile or other electronic means including, without limitation, SeamlessDocs or other City-approved program, Tagged Image Format Files (TIFF), or Portable Document Format (PDF).

26. **Conflict in Terms.** In the event of a conflict between the terms of this Agreement and the terms in any other document, including but not limited to all Exhibits hereto, the terms of this Agreement shall prevail.

Exhibit A: Scope of Services
Exhibit B: Compensation Schedule
Exhibit C: Service Level Agreement (SLA)
Exhibit D: City of Tukwila Security Requirements
Exhibit E: Data Protection and Information Security Exhibit

18

CITY OF TUKWILA

CONTRACTOR:

By: _____

_____
Thomas McLeod, Mayor

Printed Name: _____

_____
Date

Title: _____

Address: _____

_____

ATTEST/AUTHENTICATED:

Date: _____

_____
Andy Youn, City Clerk

APPROVED AS TO FORM:

_____
Office of the City Attorney

EXHIBIT A

Scope of Services

GRANICUS

Granicus Proposal for Tukwila, WA

ORDER DETAILS

Prepared By:	Taylor Brodersen
Phone:	(814) 720-4368
Email:	taylor.brodersen@granicus.com
Order #:	Q-384417
Prepared On:	18 Mar 2025
Expires On:	31 Dec 2024

ORDER TERMS

Currency:	USD
Payment Terms:	Net 30 (Payments for subscriptions are due at the beginning of the period of performance.)
Period of Performance:	The term of the Agreement will commence on the date this document is signed and will continue for 12 months.

PRICING SUMMARY

The pricing and terms within this Proposal are specific to the products and volumes contained within this Proposal.

One-Time Fees			
Solution	**Billing Frequency**	**Quantity/Unit**	**One-Time Fee**
SmartGov Training	Upon Delivery	1 Each	$2,896.00
SmartGov Custom Implementation	Upon Delivery	1 Each	$0.00
BlueBeam Connector Configuration	Upon Delivery	1 Each	$1,500.00
Project Management - SmartGov	Upon Delivery	1 Each	$8,447.85
Map Connector Configuration	Upon Delivery	1 Each	$1,250.00
Parcel Connector Configuration	Upon Delivery	1 Each	$3,125.00
Portal Configuration	Upon Delivery	1 Each	$1,250.00
Fees Configuration (Pages)	Upon Delivery	8 Each	$4,248.00
General Config	Upon Delivery	1 Each	$2,500.00
Workflow template customization	Upon Delivery	1 Each	$10,050.00
Standardized Data Migration - Permits	Upon Delivery	1 Each	$5,000.00
Base Standardized Migration Cost	Upon Delivery	1 Each	$1,875.00
Data Migration - Documents & Attachments	Upon Delivery	1 Each	$3,000.00
Standardized Data Migration - Code Enforcement	Upon Delivery	1 Each	$3,125.00
Standardized Data Migration - Licensing	Upon Delivery	1 Each	$6,250.00
Contractor Connector Configuration	Upon Delivery	1 Each	$1,250.00
Financial Export Connector Configuration	Upon Delivery	1 Each	$2,500.00
Existing Merchant Connector Configuration	Upon Delivery	1 Each	$1,500.00
Laserfiche Connector Configuration	Upon Delivery	1 Each	$3,125.00
Active Directory Connector Configuration	Upon Delivery	1 Each	$1,875.00
		SUBTOTAL:	**$64,766.85**

New Subscription Fees

Solution	Billing Frequency	Quantity/Unit	Annual Fee
SmartGov - Enterprise	Annual	1 Each	$27,424.00
SmartGov Code Enforcement	Annual	1 Each	$0.00
SmartGov Licensing	Annual	1 Each	$0.00
SmartGov Permitting	Annual	1 Each	$0.00
SmartGov Connector BlueBeam	Annual	1 Each	$1,372.00
SmartGov Connector Contractor	Annual	1 Each	$1,372.00
SmartGov Connector Financial	Annual	1 Each	$1,372.00
SmartGov Connector Merchant	Annual	1 Each	$1,372.00
SmartGov API	Annual	1 Each	$2,915.00
SmartGov Connector ECM-Laserfiche	Annual	1 Each	$1,372.00
SmartGov Connector Active Directory	Annual	1 Each	$1,372.00
		SUBTOTAL:	$38,571.00

PRODUCT DESCRIPTIONS

Solution	Description
SmartGov - Enterprise	Annual subscription to SmartGov software for: Permitting, Licensing, and Code Enforcement. Subscription includes the Public Portal.
SmartGov Code Enforcement	Annual subscription for SmartGov Code Enforcement Module for managing service requests and complaints.
SmartGov Licensing	Annual subscription for SmartGov Licensing Module for contractor registration, rental registration, business licensing.
SmartGov Permitting	Annual subscription for SmartGov Permitting Module for building and planning permits, inspections, and contacts.
SmartGov Connector BlueBeam	The SmartGov Bluebeam connector provides the ability to check out documents for plan review and markup using the subscriber's Bluebeam subscription. Bluebeam Studio is the repository for Bluebeam Projects and Sessions. Only one license/subscription is required for each jurisdiction.
SmartGov Training	Includes up to two (2) hours of User Acceptance Training to prepare primary users for Validation, focused on navigation and testing best practices. Go-Live training will span a one (1) week period, provided in three (3) hour sessions focused on Permit/Application Intake, Review, Inspections and Code Enforcement processes (as needed).
SmartGov Custom Implementation	SmartGov Configuration based on implementation options selected.

Solution	Description
BlueBeam Connector Configuration	Assist Subscriber in configuring Bluebeam connection. Testing connection with Subscriber. Training provided on SmartGov check-out and check-in process only. The service and subscription for this connector does NOT include a subscription to Bluebeam or training on how to install or use the Bluebeam software. Subscriber is responsible for providing an active subscription to Bluebeam Studio Prime with REVU 21 to use the SmartGov Bluebeam Connector. Each user that will be checking permits out to Bluebeam from SmartGov or accessing the submittal documents from SmartGov for review in Bluebeam will need to be a member of the Studio Prime account. Bluebeam Software is comprised of a document management component, known as Studio, and a client-side application, Revu. Each component has three (3) editions with various features. Bluebeam Studio is the repository for Bluebeam Projects and Sessions. Only one license/subscription is required for each jurisdiction. It is available in the following editions: Bluebeam Studio Prime (Compatible with SmartGov) – Cloud-based (allows third party integrations with the Bluebeam Studio API), additional Bluebeam cost Bluebeam Studio (Not Compatible with SmartGov) – Cloud-based, included with the Bluebeam Revu user license at no additional Bluebeam cost Bluebeam Studio Enterprise (Not Compatible with SmartGov) – On-Premises Bluebeam Revu is the client-side software that provides the tools necessary to review and mark up documents. This software must be installed on each client computer that will be used to perform review and mark up tasks. Revu is available in the following editions: Revu Standard (Compatible with SmartGov) – Standard tool set Revu CAD (Compatible with SmartGov) – Includes all of the standard tools, along with plugins for 2D and 3D PDF creation Revu eXtreme (Compatible with SmartGov) – Includes all of the standard tools and CAD plugins, with additional features like Optical Character Recognition (OCR) and batch processes. The Revu user license includes access to Bluebeam Studio, but Bluebeam Studio is not sufficient for integration with SmartGov. Each SmartGov user that will be checking projects in and out of Bluebeam or performing review and mark up tasks must also be a member of the Bluebeam Studio Prime

Solution	Description
	account.
Project Management - SmartGov	Project Management: Company Project Manager will act as an extension of the Subscriber's team and manage the implementation from start to finish. The Subscriber will have access to a personalized timeline which will be reviewed on a regular cadence. The Project Manager will partner with the Subscriber to coordinate all services, management of the project timeline, and help identify risks and/or issues. Project Management Services include: • Project planning and kickoff meetings. • Project schedule developed and maintained according to the SOW tasks, deliverables, dependencies, and resource assignments. • Status reporting and coordination of status meetings, bi-weekly, or as required. • Schedule monitoring and scope management. • Risk Management planning to identify, analyze, and mitigate risks. • Action Item and decision tracking, as well as resolving and escalating issues. • Change control management and issue tracking. • Company project resource management. • Verify product and deliverable acceptance with Subscriber. • Facilitating transition to Support. • Company's Project Manager will serve as the single point of contact for the project related to this SOW.

Solution	Description
Map Connector Configuration	Configure subscribers ESRI GIS layers into SmartGov Troubleshooting the incoming data Train client on how to maintain the service in SmartGov. MAP/GIS Connector: Company will connect to ESRI Map Service provided by Subscriber and secured by a publicly trusted certificate issued by a Certificate Authority. Subscriber is responsible for contracting separately with ESRI map service provider and ESRI configuration. SmartGov Requirements for Map Connector Integration: ArcGIS for Server 10.4 or ArcGIS for server Enterprise Standard 10.7.1 (OR) ArcGIS Online. Subscriber Map Service must be publicly accessible and require no user authentication of any kind. The Map Service must include a parcel layer with a designated field having parcel numbers that exactly match those provided in the Parcel Connector source data (this layer may be the same as that provided for the Parcel Connector if no authentication is required for access). Support for Feature, Tiled, and Web Map Services is not included. Custom base maps are not supported. Base maps from the ESRI base map library will be available for use. The following base maps are currently included (subject to change): Imagery Imagery Hybrid Streets Topographic Navigation Streets (Night) Terrain with Labels Light Gray Canvas Dark Gray Canvas Oceans National Geographic Style Map Open Street Map Charted Territory Map Community Map Navigation (Dark Mode) Newspaper Map Human Geography Map Human Geography Dark Map Modern Antique Map Mid-Century Map Nova Map Colored Pencil Map Firefly Imagery Hybrid

Solution	Description
	USA Topo Maps

Solution	Description
Parcel Connector Configuration	Company will configure EITHER a Delimited Parcel Job OR ARCGIS Parcel Job on behalf of the Subscriber. Configure Subscribers parcel fields into SmartGov. Troubleshooting the incoming data and providing recommendations for Subscriber to resolve data gaps. Train Subscriber on how to maintain the service in SmartGov. Delimited File – A delimited file may be uploaded to the job at runtime. The delimited file option supports a single address for each individual parcel. Subscriber must use the template provided by Company. Parcel Layer – A parcel layer must be accessible by URL through an ESRI REST service. A secondary address-only layer may also be provided for parcels that have more than one address. The layer(s) must be publicly accessible and may be secured with a username and password. Subscriber is responsible for obtaining, cleaning, and maintaining all parcel data within the delimited file and/or ESRI Rest service. The configured parcel job will be available for Subscriber to run on-demand after go-live. The Parcel Layer Job can be set to run daily, weekly, monthly, or annually defined by how often Subscriber intends to update the Rest Service. Parcel source data (delimited file or parcel layer) must include the following fields, at a minimum: Parcel Number Primary Situs Address Primary Situs City Primary Situs State Primary Situs Zip Code Owner Name Owner Street Address Owner City populated for USA addresses only Owner State populated for USA addresses only Owner Zip Code populated for USA addresses only International Indicator with a value of "Y" for any owner address outside of the USA International line including the full regional equivalent of the city, state and zip code for any owner address outside of the USA Inclusion of the following additional fields is recommended: Parcel center point latitude in decimal degrees Parcel center point longitude in decimal degrees If using a secondary address layer with the ARCGIS Parcel job, the address layer must contain the following fields: Parcel Number

Solution	Description
	Secondary Situs Address Secondary Situs City Secondary Situs Zip Code Inclusion of the following additional fields is recommended for the secondary address layer: Address point latitude in decimal degrees Address point longitude in decimal degrees
Portal Configuration	Company will customize Subscriber's Portal by: • Loading Subscriber logo. • Exposing all permits/business licenses identified in Configuration workbook in which citizens will have access. • Advising on best practices for public release timeline and access code configuration. • Load Subscriber custom verbiage into limited fields. • Provide the access URL (Uniform Resource Locator) for Subscriber to add link to jurisdiction web pages. Includes consultant-led end-to-end walkthrough and demonstration of UAT/Validation process to Subscriber to confirm functionality meets configuration requirements.
Fees Configuration (Pages)	Subscriber Fees configured based on provided Fee schedule and according to Configuration Workbook. Based on Subscriber fee schedule, defined in the Order Form, Company will: • Setup Subscriber fee code calculations. • Load Subscriber FMS (Financial Management System) / GL (General Ledger Code) (according to Configuration Workbook). • Load Subscriber Valuation table (according to Configuration Workbook or ICC (International Chamber of Commerce) table). Setup Subscriber fixture costs (according to Configuration Workbook). • Load other Subscriber custom attributes / details as required for Subscriber fee calculations (according to Configuration Workbook).

Solution	Description
General Config	General Configuration: As part of the General Configuration, Company will: • Create Subscriber database with best practice defaults. • Provide Validation environment access to Subscriber. • Load Subscriber users with Company standard permissions (according to Configuration Workbook). • Configure system values (locality, time zone, header and footer detail, standard report settings). • Load Client Code References/Violation types (according to Configuration Workbook). • Set up General Ledger accounts. • Load Subscriber logo. • Provide access to over 100 reports and output document templates. Subscriber receives credentials for environment when initial configuration items under General Configuration deliverable are completed.
Workflow template customization	Workflow Template Configuration: Company will configure process templates as defined in the Business Process Analysis phase for each department in scope: Building/Permits, Code Enforcement, Licensing and/or Recurring Inspections. Company will: Load Subscriber Code References/Violation types (according to Configuration Workbook). Load custom attributes/details within the limited fields available (not associated with fees, according to Configuration Workbook). Configure workflow to meet business requirements defined in Configuration Workbook. Consultant-led end-to-end walkthrough and demonstration of UAT/Validation process to Subscriber to confirm functionality meets configuration requirements. Completed upon configuration according to documentation in the Configuration Workbook Percentage: 100%

Solution	Description
Standardized Data Migration - Permits	Company will import permit data from a single client database source, approved by Company as standard source data. Multiple databases or unapproved source data will be subject to a change order for a custom data migration. The fields below are considered in-scope of a standard Permit data migration. The final output has many factors, including the fields available from the source data. Fields: Basic Permit Info, Parcel Contacts (Contractors will be listed on Contacts), Inspections, Fees as Notes, Notes The data migration process assumptions: Subscriber will provide an initial data set from source database. Company will provide a mapping workbook to Subscriber where Subscriber is responsible for mapping data fields to the preconfigured database fields. Subscriber will have two (2) weeks ten (10) business days to validate the initial data load and provide feedback. There is a maximum of two (2) rounds of feedback within that 10-day period. Thorough validation is necessary for any successful SmartGov data migration as there is no additional data cleansing possible after the final migration. No more system changes will be permitted after successful Validation. Subscriber to provide a final data set three (3) business days before Go-Live. Final data load will occur the day before Go-Live.

Solution	Description
Base Standardized Migration Cost	Base Data Migration includes non-module data such as contacts and is included in all standard data migration packages with one or more module data migrations. Company will import permit data from a single client database source, approved by Company as standard source data. Multiple databases or unapproved source data will be subject to a change order for a custom data migration. The Standard Data Migration includes the Base fields and one or more of the additional datasets per the Sales Order Form. The fields below are considered in-scope of a standard data migration. The final output has many factors, including the fields available from the source data. Parcels: Ownership Addresses Contacts: Phone Address Email The data migration process assumptions: Subscriber will provide an initial data set from source database. Company will provide a mapping workbook to Subscriber where Subscriber is responsible for mapping data fields to the preconfigured database fields. Subscriber will have two (2) weeks ten (10) business days to validate the initial data load and provide feedback. There is a maximum of two (2) rounds of feedback within that 10-day period. Thorough validation is necessary for any successful SmartGov data migration as there is no additional data cleansing possible after the final migration. No more system changes will be permitted after successful Validation. Subscriber to provide a final data set three (3) business days before Go-Live. Final data load will occur the day before Go-Live.
SmartGov Connector Contractor	Contractor Connector links to state database to verify licenses and update contractor license information automatically. Alternatively, SmartGov Contractor Connector provides a one-time CSV upload that may include data out of scope of the standard contact-contractor upload.
SmartGov Connector Financial	The SmartGov Financial Connector outputs a financial extract with a pre-determined format which may be written to the customer's FTP site, if desired, to facilitate automated external processing of the file. The customer may request the use of an alternate delimiter if a comma is not acceptable. The financial extract job may be run on demand or scheduled to run on a consistent basis (e.g., daily, weekly, monthly, etc.). Companion reports designed for reconciliation and extract verification are also available.
SmartGov Connector Merchant	Connection to one merchant in the back office and/or portal from a list of available options. Subscriber remains responsible for the relationship with the provider.

Solution	Description
Data Migration - Documents & Attachments	Includes migration of clients documents/images as attachments to notes on permits, parcels, code enforcement cases or licenses. Client must provide easy mapping from documents to the object (permit, parcel, case etc...) it will be attached to
Standardized Data Migration - Code Enforcement	Company will import Code Enforcement data from a single client database source, approved by Company as standard source data. Multiple databases or unapproved source data will be subject to a change order for a custom data migration. The fields below are considered in-scope of a standard Code Enforcement data migration. The final output has many factors, including the fields available from the source data. Migration includes only current occurrence, no history. Fields: Case Request, Basic Case, Info Complainant, Contacts, Inspections, Fees as Notes, Notes The data migration process assumptions: Subscriber will provide an initial data set from source database. Company will provide a mapping workbook to Subscriber where Subscriber is responsible for mapping data fields to the preconfigured database fields. Subscriber will have two (2) weeks ten (10) business days to validate the initial data load and provide feedback. There is a maximum of two (2) rounds of feedback within that 10-day period. Thorough validation is necessary for any successful SmartGov data migration as there is no additional data cleansing possible after the final migration. No more system changes will be permitted after successful Validation. Subscriber to provide a final data set three (3) business days before Go-Live. Final data load will occur the day before Go-Live.

Solution	Description
Standardized Data Migration - Licensing	Company will import Licensing data from a single client database source, approved by Company as standard source data. Multiple databases or unapproved source data will be subject to a change order for a custom data migration. The fields below are considered in-scope of a standard Licensing data migration. The final output has many factors, including the fields available from the source data. Migration includes only current occurrence, no history. Fields: License Info, Contacts, Parcels, Inspections, Fees as Notes, Notes The data migration process assumptions: Subscriber will provide an initial data set from source database. Company will provide a mapping workbook to Subscriber where Subscriber is responsible for mapping data fields to the preconfigured database fields. Subscriber will have two (2) weeks ten (10) business days to validate the initial data load and provide feedback. There is a maximum of two (2) rounds of feedback within that 10-day period. Thorough validation is necessary for any successful SmartGov data migration as there is no additional data cleansing possible after the final migration. No more system changes will be permitted after successful Validation. Subscriber to provide a final data set three (3) business days before Go-Live. Final data load will occur the day before Go-Live.

Solution	Description
Contractor Connector Configuration	Import of contractors from a delimited file or a SODA query (Washington and Arizona clients only). SODA Imports. Includes completed configuration of field mapping and credential link. The states of Washington and Arizona have access to a SODA load which will be configured according to existing keys. This runs on a scheduled recurrence. Delimited File Imports. The contractor data load is a one-time delimited file import. Future additions and changes to contractor information will be managed through manual updates in SmartGov. The Subscriber is responsible for any data cleansing and parsing. Includes: .csv data load (one-time data load) Provide Subscriber a .csv file to be completed by Subscriber. Configure to Subscriber's provided fields. Troubleshoot errors and provide Subscriber guidance on resolutions that Subscriber will need to resolve within the file. Delimited File Import Required fields below: Contractor Display Name Contractor Address Contractor City Contractor State Contractor Zip Contractor License Number License Type License Exp. D

Solution	Description
Financial Export Connector Configuration	Configure financial export according to subscribers FMS (financial management system) as provided by Subscriber. Train Subscriber on how to export and set scheduler. Company will customize the configuration of the export to match Subscriber financial system input needs as documented. Available customizations include: Additional data fields Altered order of column information Alternate delimiter or fixed width formatting A header line is not part of the export. Financial Connector does not connect directly with any Financial Management System. If Subscriber provides a local (FTP) File Transfer Protocol, the Financial Connector can automatically upload to the defined FTP destination. By default, financial extract jobs are pre-configured and the included configuration of the Receipt Extract job will produce a comma-delimited file with the following data points: Receipt Number Receipt Date FMS/GL Code Fund GL Account Fee Amount Paid Fee Code Name Permit/License/Case Number Payer Name The included configuration of the Receipt Extract – FMS/GL Summary job will produce a comma-delimited file with the following data points: FMS/GL Code Fund GL Account Fee Amount Paid The file output of the financial extract may be written to the customer's FTP site, if desired, to facilitate automated external processing of the file. The customer may request the use of an alternate delimiter if a comma is not acceptable. The financial extract job may be run on demand or scheduled to run on a consistent basis (e.g., daily, weekly, monthly, etc.). Companion reports designed for reconciliation and extract verification are also available.

Solution	Description
Existing Merchant Connector Configuration	Configure merchant connection. Test and troubleshoot connection during test process. Subscriber to provide the required linking information for Company to complete the setup. These will often include connection URLs, Login IDs, and Transaction Keys. Requirements vary slightly depending on the selected Merchant. SmartGov will not test in Production environments.
SmartGov API	SmartGov API includes standard REST API Endpoints with documentation. The following information can be requested from SmartGov: Case assignments: All inspections and code enforcement cases assigned to a person Contact, Parcel and Custom Details, Inspections, Associations, attached photos, documents, and plans on Permits, Licenses, Recurring Inspections and Code Enforcement Cases with additional information available for: - Permits - Contractor license status, conditions - Licenses - Activities, conditions - Code enforcement Cases - Workflow, Items, Violations, Citations Parcel information including Lat/Long, situs address and parcel number Contact information such as name, phone number, email, address The following information can be updated: All inspection information including assignment, requesting, scheduling, inspection status (pass/fail) and results and adding photos and notes Code enforcement case information including workflow, details, notes and attachments contact names, addresses, emails, phone numbers, points of contact The following information can be created: Contacts Inspections, including creation of inspection actions, corrections and code references, notes Code enforcement case requests Code enforcement cases including violations, citations, details, workflow steps and inspections on the case Financial specific endpoints:Obtain fees due on licenses, permits, code enforcement cases and recurring inspections Apply payments to pending receipts
SmartGov Connector ECM-Laserfiche	Laserfiche connector allows file attachments in SmartGov to be stored within Laserfiche, an ECM (Enterprise Content Management) system. The Laserfiche integration was built in compliance with CMIS (Content Management Interoperability Services) standards. Subscriber must have the Laserfiche CMIS Gateway, version 10 or higher, installed and configured for the desired repository and be able to provide a browser binding URL that SmartGov can reach from the cloud. The service and subscription for this connector does NOT include a subscription to Laserfiche or training on how to install or use the Laserfiche software.

Solution	Description
Laserfiche Connector Configuration	This connector allows file attachments in SmartGov to be stored within an ECM (Enterprise Content Management) system. The Laserfiche integration was built in compliance with CMIS (Content Management Interoperability Services) standards. Subscriber must have the Laserfiche CMIS Gateway, version 10 or higher, installed and configured for the desired repository and be able to provide a browser binding URL that SmartGov can reach from the cloud. The service and subscription for this connector does NOT include a subscription to Laserfiche or training on how to install or use the Laserfiche software. There are three Secured Functions that control access to the Laserfiche configuration options: Admin.JurisdictionBlobProvider – Allow user to all ECM settings and mappings Admin.JurisdictionBlobProvider.ConfigureCMISConnection – Allow user to configure CMIS connection settings Admin.JurisdictionBlobProvider.ConfigureECMTemplates – Allow user to configure metadata template mappings Configure Subscriber's credentials and mapping in SmartGov. Meet with Subscriber and guide them through SmartGov to test the connection.
SmartGov Connector Active Directory	Connector for integration with Active Directory. SmartGov Requirements for integration with Active Directory: ADFS (Active Directory Federation Services) version 5.0 or higher (Windows server 2019 or higher). Mobile ADFS in Azure to support PKCE (Proof Key for Code Exchange) for OAuth 2.0 Azure AD expires every 24-months and the Subscriber has to maintain their secret keys in Production. For SSO (Single Sign On) SAML v2
Active Directory Connector Configuration	Configure Subscribers credentials in SmartGov. Meet with Subscribers and guide through the connection in SmartGov for testing and maintaining. Subscriber is responsible for the installation and configuration of active directory technology.

TERMS & CONDITIONS

- This quote, and all products and services delivered hereunder are governed by the terms located at https://granicus.com/legal/licensing, including any product-specific terms included therein (the "License Agreement"). If your organization and Granicus has entered into a separate agreement or is utilizing a contract vehicle for this transaction, the terms of the License Agreement are incorporated into such separate agreement or contract vehicle by reference, with any directly conflicting terms and conditions being resolved in favor of the separate agreement or contract vehicle to the extent applicable.

- If submitting a Purchase Order, please include the following language: The pricing, terms and conditions of quote Q-384417 dated 18 Mar 2025 are incorporated into this Purchase Order by reference and shall take precedence over any terms and conditions included in this Purchase Order.

- This quote is exclusive of applicable state, local, and federal taxes, which, if any, will be included in the invoice. It is the responsibility of Tukwila, WA to provide applicable exemption certificate(s).

- Any lapse in payment may result in suspension of service and will require the payment of a setup fee to reinstate the subscription.

BILLING INFORMATION

Billing Contact:		Purchase Order Required?	[ ] - No [ ] - Yes
Billing Address:		PO Number: *If PO required*	
Billing Email:		Billing Phone:	

If submitting a Purchase Order, please include the following language:
The pricing, terms, and conditions of quote Q-384417 dated 18 Mar 2025 are incorporated into this Purchase Order by reference and shall take precedence over any terms and conditions included in this Purchase Order.

AGREEMENT AND ACCEPTANCE

By signing this document, the undersigned certifies they have authority to enter the agreement. The undersigned also understands the services and terms.

Tukwila, WA	
Signature:	
Name:	
Title:	
Date:	

EXHIBIT B

Compensation Schedule

GRANICUS

Granicus Proposal for Tukwila, WA

ORDER DETAILS

Prepared By:	Taylor Brodersen
Phone:	(814) 720-4368
Email:	taylor.brodersen@granicus.com
Order #:	Q-384417
Prepared On:	18 Mar 2025
Expires On:	31 Dec 2024

ORDER TERMS

Currency:	USD
Payment Terms:	Net 30 (Payments for subscriptions are due at the beginning of the period of performance.)
Period of Performance:	The term of the Agreement will commence on the date this document is signed and will continue for 12 months.

PRICING SUMMARY

The pricing and terms within this Proposal are specific to the products and volumes contained within this Proposal.

One-Time Fees			
Solution	**Billing Frequency**	**Quantity/Unit**	**One-Time Fee**
SmartGov Training	Upon Delivery	1 Each	$2,896.00
SmartGov Custom Implementation	Upon Delivery	1 Each	$0.00
BlueBeam Connector Configuration	Upon Delivery	1 Each	$1,500.00
Project Management - SmartGov	Upon Delivery	1 Each	$8,447.85
Map Connector Configuration	Upon Delivery	1 Each	$1,250.00
Parcel Connector Configuration	Upon Delivery	1 Each	$3,125.00
Portal Configuration	Upon Delivery	1 Each	$1,250.00
Fees Configuration (Pages)	Upon Delivery	8 Each	$4,248.00
General Config	Upon Delivery	1 Each	$2,500.00
Workflow template customization	Upon Delivery	1 Each	$10,050.00
Standardized Data Migration - Permits	Upon Delivery	1 Each	$5,000.00
Base Standardized Migration Cost	Upon Delivery	1 Each	$1,875.00
Data Migration - Documents & Attachments	Upon Delivery	1 Each	$3,000.00
Standardized Data Migration - Code Enforcement	Upon Delivery	1 Each	$3,125.00
Standardized Data Migration - Licensing	Upon Delivery	1 Each	$6,250.00
Contractor Connector Configuration	Upon Delivery	1 Each	$1,250.00
Financial Export Connector Configuration	Upon Delivery	1 Each	$2,500.00
Existing Merchant Connector Configuration	Upon Delivery	1 Each	$1,500.00
Laserfiche Connector Configuration	Upon Delivery	1 Each	$3,125.00
Active Directory Connector Configuration	Upon Delivery	1 Each	$1,875.00
		SUBTOTAL:	**$64,766.85**

New Subscription Fees

Solution	Billing Frequency	Quantity/Unit	Annual Fee
SmartGov - Enterprise	Annual	1 Each	$27,424.00
SmartGov Code Enforcement	Annual	1 Each	$0.00
SmartGov Licensing	Annual	1 Each	$0.00
SmartGov Permitting	Annual	1 Each	$0.00
SmartGov Connector BlueBeam	Annual	1 Each	$1,372.00
SmartGov Connector Contractor	Annual	1 Each	$1,372.00
SmartGov Connector Financial	Annual	1 Each	$1,372.00
SmartGov Connector Merchant	Annual	1 Each	$1,372.00
SmartGov API	Annual	1 Each	$2,915.00
SmartGov Connector ECM-Laserfiche	Annual	1 Each	$1,372.00
SmartGov Connector Active Directory	Annual	1 Each	$1,372.00
		SUBTOTAL:	$38,571.00

EXHIBIT C

SERVICE LEVEL AGREEMENT (SLA)

Service Level Agreement: The Services, in a production environment, are provided with the service levels described in this Exhibit ___. SLAs are only applicable to production environments. SLAs will be available upon Customer's signature of Contractor's Go Live Acceptance Form for Customer's production environment.

"Contractor" means [_____].

99.9% Application Availability

Actual Application Availability % = (Monthly Minutes (MM) minus Total Minutes Not Available (TM)) multiplied by 100) and divided by Monthly Minutes (MM), but not including Excluded Events

Service Credit Calculation: An Outage will be deemed to commence when the Applications are unavailable to Customer in Customer's production environment hosted by Contractor and end when Contractor has restored availability of the Applications.   Failure to meet the 99.9% Application Availability SLA, other than for reasons due to an Excluded Event, will entitle Customer to a credit as follows:

Actual Application Availability % (as measured in a calendar month)	Service Credit to be applied to Customer's monthly invoice for the affected month
<99.9% to 99.75%	10%
<99.75% to 98.25%	15%
<98.25% to 97.75%	25%
<97.75% to 96.75%	35%
<96.75%	50%

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

"Excluded Event" means any event that results in an Outage and is caused by: (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 Contractor, including without limitation Customer Content, failures or malfunctions resulting from circuits provided by Customer, any inconsistencies or changes in Customer's source environment, including either intentional or accidental connections or disconnections to the environment; (c) Force Majeure events; (d) expected downtime during the Maintenance Periods described below; (e) any suspension of the Services in accordance with the terms of the Agreement to which this Exhibit C is attached; (f) the unavailability of required Customer personnel, including as a result of failure to provide Contractor with accurate, current contact information; or (g) using an Application in a manner inconsistent with the Documentation for such Application.

"Maintenance Period" means scheduled maintenance periods established by Contractor to maintain and update the Services, when downtime may be necessary, as further described below. The Maintenance Period is used for purposes of the Service Credit Calculation; Contractor continuously maintains the production environment on a 24x7 basis to reduce disruptions.

Customer Specific Maintenance Period

1. Customer will choose one of the following time zones for their Maintenance Period:
   a. United States Eastern Standard Time,
   b. GMT/UTC,
   c. Central European Time (CET) or
   d. Australian Eastern Standard Time (AEST).

2. Customer will choose one of the following days of the week for their Maintenance Period: Saturday, Sunday, Wednesday or Thursday.

3. Contractor will use up to 6 hours in any two consecutive rolling months (specifically: January and February; March and April; May and June; July and August; September and October; November and December) to perform Customer Specific Maintenance, excluding any customer requested Application updates. Downtime in excess of these six hours will be deemed to be an Outage.

4. Customer Specific Maintenance will occur between 12 am - 6 am during Customer's selected time zone.

5. Excluding any customer requested Application updates, Contractor will provide notice for planned downtime via an email notice to the primary Customer contact at least seven days in advance of any known downtime so planning can be facilitated by Customer.

6. Customer Specific Maintenance Windows also include additional maintenance windows mutually agreed upon by Customer and Contractor.

7. In absence of instruction from Customer, Contractor will by default perform Maintenance in the time zone where the Data Center is located.

Non-Customer Specific Maintenance Period

Contractor anticipates non-Customer Specific Maintenance to be performed with no or little (less than three hours per month) Customer downtime. If for any reason non-Customer Specific Maintenance requires downtime, Contractor will provide as much notice as reasonably possible of the expected window in which this will occur. Downtime in excess of three hours per month for Non-Customer Specific Maintenance will be deemed to be an Outage.

"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 Services are unavailable as the result of an Outage.

Reporting and Claims Process: Service Credits will not be provided if: (a) Customer is in breach or default under the Agreement at the time the Outage occurred; or (b) the Outage results from an Excluded Event.

Contractor will provide Customer with an Application Availability report on a monthly basis for each prior calendar month. Within 60 days of receipt of such report, Customer must request the applicable Service Credit by written notice to Contractor. Customer waives any right to Service Credits not requested within this time period. All performance calculations and applicable Service Credits are based on Contractor records and data unless Customer can provide Contractor with clear and convincing evidence to the contrary.

The Service Level Agreements in this Exhibit, and the related Service Credits, apply on a per production environment basis. For the avoidance of doubt, Outages in one production environment may not be added to Outages in any other production environment for purposes of calculating Service Credits.

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

Exhibit D
City of Tukwila Security Requirements

Introduction

During the term of this agreement, Contractor shall operate an information security program designed to meet the confidentiality, integrity, and availability requirements of the service or product being supplied. The program shall include at a minimum the following security measures.

Governance

1. ***Information Security Policy:*** Contractor shall develop, implement, and maintain an information security policy and shall communicate the policy to all staff and contractors.

2. ***Information Security Accountability:*** Contractor shall appoint an employee of at least manager level who shall be accountable for the overall information security program.

3. ***Risk Management:*** Contractor shall employ a formal risk assessment process to identify security risks which may impact the products or services being supplied, and mitigate risks in a timely manner commensurate with the risk.

Asset Management

4. ***Asset Inventory:*** Contractor shall maintain an inventory of all hardware and software assets, including asset ownership.

5. ***Data Classification:*** Contractor shall develop, implement, and maintain a data classification scheme and process designed to ensure that data is protected according to its confidentiality requirements.

Supply Chain Risk Management

6. ***Supplier Security Assessments:*** Contractor shall engage in appropriate due diligence assessments of potential suppliers which may impact the security of the services or products being supplied.

7. ***Security in Supplier Agreements:*** Contractor shall ensure that agreements with suppliers who may impact the security of the services or products being supplied contain appropriate security requirements.

Human Resource Security

8. ***Information Security Awareness:*** Contractor shall develop and implement an information security awareness program designed to ensure that all employees and contractors receive security education as relevant to their job function.

9. ***Background Checks:*** Contractor shall conduct appropriate background checks on all new employees based on the sensitivity of the role that they are being hired for.

Identity Management, Authentication and Access Control

10. ***Authentication:*** Contractor shall ensure that all access, by employees or contractors, to its information systems used to provide services or products being supplied shall require appropriate authentication controls that at a minimum will include:

a. Strong passwords or multi-factor authentication for users

b. Multi-factor authentication for all remote access

11. ***Authorization:*** Contractor shall ensure that all access to its information systems used to provide services or products being supplied shall be approved by management.

12. ***Privileged Account Management:*** Contractor shall appropriately manage and control privileged accounts on its information systems that at a minimum will include:

a. Use of dedicated accounts for privileged activity

b. Maintaining an inventory of privileged accounts

13. ***Access Termination:*** Contractor shall develop and maintain a process designed to ensure that user access is revoked upon termination of employment, or contract for contractors.

Data Security

14. ***Encryption:*** Contractor shall ensure that all laptops, mobile devices, and removable media, including those that are owned by Contractor employees or contractors, which may be used to store, process, or transport organizational data are encrypted at all times. [Scoping guideline: This requirement may be removed if Contractor is not expected to possess any confidential or sensitive organizational data]

15. ***Secure Disposal:*** Contractor shall ensure that all media which may be used to store, process, or transport organizational data is disposed of in a secure manner. [Scoping guideline: This requirement may be removed if Contractor is not expected to possess any confidential or sensitive organizational data]

System Acquisition, Development and Maintenance

16. ***Security Requirements:*** Contractor shall ensure that information security requirements are defined for all new information systems, whether acquired or developed.

17. ***Separation of Environments:*** Contractor shall ensure that development and testing environments are separate from their production environment.

18. ***Data Anonymization:*** Contractor shall ensure that the City of Tukwila's data will not be used in the development or testing of new systems unless the data is appropriately anonymized.

19. ***Secure Coding:*** Contractor shall ensure that all applications are developed with secure coding practices, including OWASP Top 10 Most Critical Web Application Security Risks.

Physical and Environmental Security

20. ***Risk Assessment:*** Contractor shall use a formal risk assessment methodology to identify physical and environmental threats and shall implement controls to minimize the risks.

50

Information Protection Processes and Procedure

21. ***Hardening:*** Contractor shall develop and implement security configuration baselines for all endpoint and network devices types.

22. ***Network Segregation:*** Contractor shall segregate its network into zones based on trust levels, and control the flow of traffic between zones.

23. ***Anti-Malware:*** Contractor shall ensure that all information systems that are susceptible to malware are protected by up-to-date anti-malware software.

24. ***Wireless Access Control:*** Contractor shall ensure that wireless network access is protected, including at a minimum:

    a. All wireless network access should be encrypted

    b. All wireless network access to the production network should be authenticated using multi-factor authentication such as machine certificates

    c. Wireless network access for personal devices and guest access should be segregated from the production network

25. ***Patching:*** Contractor shall evaluate, test, and apply information system patches in a timely fashion according to their risk.

26. ***Backup and Recovery:*** Contractor shall implement a backup and recovery process designed to ensure that data can be recovered in the event of unexpected loss.

Protective Technology

27. ***Logging:*** Contractor shall ensure that security event logging requirements have been defined, and that all information systems are configured to meet logging requirements.

28. ***Intrusion Detection:*** Contractor shall deploy intrusion detection or prevention systems at the network perimeter.

29. ***URL Filtering:*** Contractor shall deploy tools to limit web browsing activity based on URL categories.

30. ***Denial of Service Protection:*** Contractor shall deploy controls to detect and mitigate denial of service attacks.

Security Continuous Monitoring

31. ***Security Monitoring:*** Contractor shall deploy automated tools to collect, correlate, and analyze security event logs from multiple sources, and monitor them for suspected security incidents.

32. ***Vulnerability Assessments:*** Contractor shall conduct vulnerability assessments against all Internet-facing information systems on a regular basis, no less often than quarterly.

33. ***Penetration Testing:*** Contractor shall perform penetration tests on all web applications and services, in accordance with standard penetration testing methodologies, on a regular basis, no less often than annually.

Information Security Incident Management

34. ***Incident Response:*** Contractor shall develop, implement, and maintain an information security incident response process, and will test the process on a regular basis, no less often than annually.

Exhibit E
Data Protection and Information Security

This Data Protection and Information Security Exhibit ("Exhibit") is an attachment to the Agreement and sets forth the data protection and information security requirements of City of Tukwila. This Exhibit includes by reference the terms and conditions of the Agreement. In the event of any inconsistencies between this Exhibit and the Agreement, the parties agree that the terms and conditions of the Exhibit will prevail. Throughout the term of the Agreement and for as long as Contractor controls, possesses, stores, transmits, or processes Confidential Information as part of the Services provided to City of Tukwila, Contractor will comply with the requirements set forth in this Exhibit. Any breach of this Exhibit will be deemed a material breach under the Agreement.

1. **Definitions**

"Authorized Personnel" for the purposes of this Exhibit, means Contractor's employees or subcontractors who: (i) have a need to receive or access Confidential Information or Personal Information to enable Contractor to perform its obligations under the Agreement; and (ii) are bound in writing with Contractor by confidentiality obligations sufficient for the protection of Confidential Information and Personal Information in accordance with the terms and conditions set forth in the Agreement and this Exhibit.

"Common Software Vulnerabilities" (CSV) are application defects and errors that are commonly exploited in software. This includes but is not limited to:

   (i)   The CWE/SANS Top 25 Programming Errors – see http://cwe.mitre.org/top25/ and http://www.sans.org/top25-software-errors/

   (ii) The Open Web Application Security Project's (OWASP) "Top Ten Project" – see http://www.owasp.org

"Confidential Information" means certain non-public proprietary information that has economic value and is protected with reasonable safeguards to maintain its secrecy. Confidential Information may include, but is not limited to any financial data, business and other plans, specifications, equipment designs, electronic configurations, design information, product architecture algorithms, quality assurance plans, inventions (whether or not the subject of pending patent applications), ideas, discoveries, formulae, models, requirements, standards, trade and manufacturing secrets, drawings, samples, devices, demonstrations, technical information, all Personal Information as defined in RCW 42.56.590 that come within the Contractor's possession in the course of performance under this Agreement, as well as any and all intellectual and industrial property rights contained therein or in relation thereto; provided that, Personal Information shall remain Confidential Information even if at the time of disclosure or collection, or later, it is or becomes known to the public.

"Industry Standards" mean generally recognized industry standards, best practices, and benchmarks including but not limited to:

   (i)   Payment Card Industry Data Security Standards ("PCI DSS") – see http://www.pcisecuritystandards.org/

   (ii) National Institute for Standards and Technology – see http://csrc.nist.gov/

   (iii) ISO / IEC 27000-series – see http://www.iso27001security.com/

(iv)   COBIT 5 – http://www.isaca.org/cobit/

(v)   Cyber Security Framework – see http://www.nist.gov/cyberframework/

(vi)   Cloud Security Alliance – see https://cloudsecurityalliance.org/

(vii)   Other standards applicable to the services provided by Contractor to City of Tukwila

"Information Protection Laws" mean all local, state, federal and international laws, standards, guidelines, policies, regulations and procedures applicable to Contractor or City of Tukwila pertaining to data security, confidentiality, privacy, and breach notification.

"Personal Information" also known as Personally Identifiable Information (PII), is defined in RCW 42.56.590 and includes information of City of Tukwila customers, employees and subcontractors or their devices gathered or used by Contractor that can be used on its own or combined with other information to identify, contact, or locate a person, or to identify an individual or his or her device in context. Examples of Personal Information include name, social security number or national identifier, biometric records, driver's license number, device identifier, IP address, MAC address, either alone or when combined with other personal or identifying information which is linked or linkable to a specific individual or device, such as date and place of birth, mother's maiden name, etc.

"Security Incident" is any actual or suspected occurrence of:

(i)   Unauthorized access, use, alteration, disclosure, loss, theft of, or destruction of Confidential Information or the systems / storage media containing Confidential Information

(ii)   Illicit or malicious code, phishing, spamming, spoofing

(iii) Unauthorized use of, or unauthorized access to, Contractor's systems

(iv)   Inability to access Confidential Information or Contractor systems as a result of a Denial of Service (DOS) or Distributed Denial of Service (DDOS) attack

(v)   Loss of Confidential Information due to a breach of security

"Security Vulnerability" is an application, operating system, or system flaw (including but not limited to associated process, computer, device, network, or software weakness) that can be exploited resulting in a Security Incident.

2. **Roles of the Parties and Compliance with Information Protection Laws**

As between City of Tukwila and Contractor, City of Tukwila shall be the principal and Contractor shall be its agent with respect to the collection, use, processing and disclosure of all Confidential Information. The Parties shall comply with their respective obligations as the principal (e.g., data owner/controller/covered entity) and agent (e.g., data processor/business associate/trading partner) under all Information Protection Laws. The Parties acknowledge that, with respect to all Confidential Information processed by Contractor for the purpose of providing the Services under this Agreement:

a. City of Tukwila shall determine the scope, purpose, and manner in which such Confidential Information may be accessed or processed by Contractor, and Contractor shall limit its access to or use of Confidential Information to that which is necessary to

provide the Services, comply with applicable laws, or as otherwise directed by City of Tukwila;

b. Each party shall be responsible for compliance with Information Protection Laws in accordance with their respective roles; and

c. Contractor and City of Tukwila shall implement the technical and organizational measures specified in this Exhibit and any additional procedures agreed upon pursuant to a Statement of Work ("SOW") to protect Confidential Information against unauthorized use, destruction or loss, alteration, disclosure or access.

3. **General Security Requirements**

Contractor will have an information security program that has been developed, implemented and maintained in accordance with Industry Standards. At a minimum, Contractor's information security program will include, but not be limited to, the following elements:

3.1 **Information Security Program Management.** Contractor will have or assign a qualified member of its workforce or commission a reputable third-party service provider to be responsible for the development, implementation and maintenance of Contractor's enterprise information security program.

3.2 **Policies and Standards.** To protect City of Tukwila Confidential Information, Contractor will implement and maintain reasonable security that complies with Information Protection Laws and meets data security Industry Standards.

a. <u>Security Policies and Standards</u>. Contractor will maintain formal written information security policies and standards that:

(i) Define the administrative, physical, and technological controls to protect the confidentiality, integrity, and availability of Confidential Information, City of Tukwila systems, and Contractor systems (including mobile devices) used in providing Services to City of Tukwila

(ii) Encompasses secure access, retention, and transport of Confidential Information

(iii) Provide for disciplinary or legal action in the event of violation of policy by employees or Contractor subcontractors and vendors

(iv) Prevent unauthorized access to City of Tukwila data, City of Tukwila systems, and Contractor systems, including access by Contractor's terminated employees and subcontractors

(v) Employ the requirements for assessment, monitoring and auditing procedures to ensure Contractor is compliant with the policies

(vi) Conduct an annual assessment of the policies, and upon City of Tukwila written request, provide attestation of compliance.

b. In the SOW or other document, Contractor will identify to City of Tukwila all third-party vendors (including those providing subcontractors to Contractor) involved in the provision of the Services to City of Tukwila, and will specify those third-party vendors that will have access to Confidential Information.

3.3 **Security and Privacy Training.** Contractor, at its expense, will train new and existing employees and subcontractors to comply with the data security and data privacy obligations under this Agreement and this Exhibit. Ongoing training is to be provided at least annually and more frequently as appropriate or requested by City of Tukwila. City of Tukwila may provide specific training material to Contractor to include in its employee/subcontractor training.

3.4 **Access Control.** Contractor will ensure that City of Tukwila Confidential Information will be accessible only by Authorized Personnel after appropriate user authentication and access controls (including but not limited to two-factor authentication) that satisfy the requirements of this Exhibit. Each Authorized Personnel shall have unique access credentials and shall receive training which includes a prohibition on sharing access credentials with any other person. Contractor should maintain access logs relevant to City of Tukwila Confidential Information for a minimum of six years or other mutually agreed upon duration.

3.5 **Data Backup.** The parties shall agree in an SOW or other document upon the categories of City of Tukwila Confidential Information that are required to be backed up by Contractor. Unless otherwise agreed to in writing by City of Tukwila, backups of City of Tukwila Confidential Information shall reside solely in the United States. For the orderly and timely recovery of Confidential Information in the event of a service interruption:

   a. Contractor will store a backup of Confidential Information at a secure offsite facility and maintain a contemporaneous backup of Confidential Information on-site to meet needed data recovery time objectives.

   b. Contractor will encrypt and isolate all City of Tukwila backup data on portable media from any backup data of Contractor's other customers.

3.6 **Business Continuity Planning (BCP) and Disaster Recovery (DR).** Contractor will maintain an appropriate business continuity and disaster recovery plan to enable Contractor to adequately respond to, and recover from, business interruptions involving City of Tukwila Confidential Information or services provided by Contractor to City of Tukwila.

   a. At a minimum, Contractor will test the BCP and DR plan annually, in accordance with Industry Standards, to ensure that the business interruption and disaster objectives set forth in this Exhibit have been met and will promptly remedy any failures. Upon City of Tukwila's request, Contractor will provide City of Tukwila with a written summary of the annual test results.

   b. In the event of a business interruption that activates the BCP and DR plan affecting the Services or Confidential Information of City of Tukwila, Contractor will notify City of Tukwila's designated Security Contact as soon as possible.

   c. Contractor will allow City of Tukwila or its authorized third party, upon a minimum of 30 days' notice to Contractor's designated Security Contact, to perform an assessment of Contractor's BCP and DR plan once annually, or more frequently if agreed to in an SOW or other document. Following notice provided by City of Tukwila, the parties will meet to determine the scope and timing of the assessment.

3.7 **Network Security.** Contractor agrees to implement and maintain network security controls that conform to Industry Standards including but not limited to the following:

a. Firewalls. Contractor will utilize firewalls to manage and restrict inbound, outbound and internal network traffic to only the necessary hosts and network resources.

b. Network Architecture. Contractor will appropriately segment its network to only allow authorized hosts and users to traverse areas of the network and access resources that are required for their job responsibilities.

c. Demilitarized Zone (DMZ). Contractor will ensure that publicly accessible servers are placed on a separate, isolated network segment typically referred to as the DMZ.

d. Wireless Security. Contractor will ensure that its wireless network(s) only utilize strong encryption, such as WPA2.

e. Intrusion Detection/Intrusion Prevention (IDS/IPS) System. Contractor will have an IDS and/or IPS in place to detect inappropriate, incorrect, or anomalous activity and determine whether Contractor's computer network and/or server(s) have experienced an unauthorized intrusion.

3.8 **Application and Software Security.** Contractor, should it provide software applications or Software as a Service (SaaS) to City of Tukwila, agrees that its product(s) will remain secure from Software Vulnerabilities and, at a minimum, incorporate the following:

a. Malicious Code Protection. Contractor's software development processes and environment must protect against malicious code being introduced into its product(s) future releases and/or updates.

b. Application Level Security. Contractor must use a reputable third party to conduct static/manual application vulnerability scans on the application(s) software provided to City of Tukwila for each major code release or at the time of contract renewal. An *internally* produced static/manual test from the Contractor will not be accepted. Results of the application testing will be provided to City of Tukwila in a summary report and vulnerabilities categorized as Very High, High or that have been identified as part of the OWASP Top 10 and SANS Top 25 within 10 weeks of identification.

c. Vulnerability Management. Contractor agrees at all times to provide, maintain and support its software and subsequent updates, upgrades, and bug fixes such that the software is and remains secure from Common Software Vulnerabilities.

d. Logging. Contractor software that controls access to Confidential Information must log and track all access to the information.

e. Updates and Patches. Contractor agrees to promptly provide updates and patches to remediate Security Vulnerabilities that are exploitable. Upon City of Tukwila's request, Contractor shall provide information on remediation efforts of known Security Vulnerabilities.

3.9 **Data Security.** Contractor agrees to preserve the confidentiality, integrity and accessibility of City of Tukwila Confidential Information with administrative, technical and physical measures that conform to Industry Standards that Contractor then applies to its own systems and processing environment. Unless otherwise agreed to in writing by City of Tukwila, Contractor agrees that any and all City of Tukwila Confidential Information will be stored, processed, and maintained solely on designated systems located in the continental United States. Additionally:

56

a. <u>Encryption</u>. Contractor agrees that all City of Tukwila Confidential Information and Personal Information will be encrypted with a Federal Information Processing Standard (FIPS) compliant encryption product, also referred to as 140-2 compliant. Symmetric keys will be encrypted with a minimum of 128-bit key and asymmetric encryption requires a minimum of 1024 bit key length. Encryption will be utilized in the following instances:

- City of Tukwila Confidential Information and Personal Information will be stored on any portable computing device or any portable storage medium.

- City of Tukwila Confidential Information and Personal Information will be transmitted or exchanged over a public network.

b. <u>Data Segregation</u>. Contractor will segregate City of Tukwila Confidential Information and Personal Information from Contractor's data and from the data of Contractor's other customers or third parties.

3.10 **Data Re-Use.** Contractor agrees that any and all data exchanged shall be used expressly and solely for the purposes enumerated in the Agreement. Data shall not be distributed, repurposed or shared across other applications, environments, or business units of Contractor. Contractor further agrees that no Confidential Information of any kind shall be transmitted, exchanged or otherwise passed to other parties except on a case-by-case basis as specifically agreed to in writing by City of Tukwila.

3.11 **Data Destruction and Data Retention.** Upon expiration or termination of this Agreement or upon City of Tukwila's written request, Contractor and its Authorized Personnel will promptly return to City of Tukwila all City of Tukwila Confidential Information and/or securely destroy City of Tukwila Confidential Information. At a minimum, destruction of data activity is to be performed according to the standards enumerated by the National Institute of Standards, Guidelines for Media Sanitization – see http://csrc.nist.gov/. If destroyed, an officer of Contractor must certify to City of Tukwila in writing within 10 business days all destruction of City of Tukwila Confidential Information. If Contractor is required to retain any City of Tukwila Confidential Information or metadata to comply with a legal requirement, Contractor shall provide notice to both the general notice contact in the Agreement as well as City of Tukwila's designated Security Contact.

3.12 **Right to Audit.** Upon a minimum of 30 days' written notice to Contractor, Contractor agrees to allow City of Tukwila or a mutually agreed upon independent third party under a Non-Disclosure Agreement to perform an audit of Contractor's policies, procedures, software, system(s), and data processing environment at City of Tukwila's expense to confirm compliance with this Exhibit. Prior to commencement of the audit, the parties will discuss the scope of the audit and the schedule. Contractor shall provide reasonable support to the audit team. Upon request Contractor will provide any relevant third party assessment reports such as SOC 2, PCI DSS Report on Compliance, or ISO 27001 certification. Unless critical issues are identified during the audit, such audits will be restricted to once in any 12 month period. If issues are identified, Contractor shall provide a remediation plan to City of Tukwila to remedy such issues at Contractor's expense.

3.13 **Security Testing.** Contractor, at its expense, will allow City of Tukwila to conduct static, dynamic, automated, and/or manual security testing on its software products and/or services, hardware, devices, and systems to identify Security Vulnerabilities on an ongoing basis. Should any vulnerabilities be discovered, Contractor agrees to notify City of Tukwila and create a mutually agreed upon remediation plan to resolve all vulnerabilities identified. City of Tukwila has the right to request or conduct additional reasonable security testing throughout the Term of the Agreement.

4. **Security Incident / Data Breach**

4.1 **Security Contact.** The individuals identified below shall serve as each party's designated Security Contact for security issues under this Agreement.

City of Tukwila Security Contact:

Name   _____

Address   _____

            _____

Phone   _____

Email   _____

Contractor Security Contact:

Name   _____

Address   _____

            _____

Phone   _____

Email   _____

58

4.2 **Requirements.** Contractor will take commercially reasonable actions to ensure that City of Tukwila is protected against any and all reasonably anticipated Security Incidents, including but not limited to:

(i) Contractor's systems are continually monitored to detect evidence of a Security Incident

(ii) Contractor has a Security Incident response process to manage and to take corrective action for any suspected or realized Security Incident

(iii) Upon request Contractor will provide City of Tukwila with a copy of its Security Incident policies and procedures. If a Security Incident affecting City of Tukwila occurs, Contractor, at its expense and in accordance with applicable Information Protection Laws, will immediately take action to prevent the continuation of the Security Incident.

4.3 **Notification.** Within eight hours of Contractor's initial awareness of a Security Incident or other mutually agreed upon time period, Contractor will notify City of Tukwila of the incident by calling by phone the City of Tukwila Security Contact(s) listed above.

4.4 **Investigation and Remediation.** Upon Contractor's notification to City of Tukwila of a Security Incident, the parties will coordinate to investigate the Security Incident. Contractor shall be responsible for leading the investigation of the Security Incident, but shall cooperate with City of Tukwila to the extent City of Tukwila requires involvement in the investigation. Contractor shall involve law enforcement in the investigation if requested by City of Tukwila. Depending upon the type and scope of the Security Incident, City of Tukwila personnel may participate in: (i) interviews with Contractor's employees and subcontractors involved in the incident; and (ii) review of all relevant records, logs, files, reporting data, systems, Contractor devices, and other materials as otherwise required by City of Tukwila.

Contractor will cooperate, at its expense, with City of Tukwila in any litigation or investigation deemed reasonably necessary by City of Tukwila to protect its rights relating to the use, disclosure, protection and maintenance of Confidential Information. Contractor will reimburse City of Tukwila for actual costs incurred by City of Tukwila in responding to, and mitigating damages caused by any Security Incident, including all costs of notice and remediation which City of Tukwila, in its sole discretion, deems necessary to protect such affected individuals in light of the risks posed by the Security Incident. Contractor will, at Contractor's own expense, provide City of Tukwila with all information necessary for City of Tukwila to comply with data breach recordkeeping, reporting and notification requirements pursuant to Information Protection Laws. Contractor will use reasonable efforts to prevent a recurrence of any such Security Incident. Additionally, Contractor will provide (or reimburse City of Tukwila) for at least one year of complimentary access for one credit monitoring service, credit protection service, credit fraud alert and/or similar services, which City of Tukwila deems necessary to protect affected individuals in light of risks posed by a Security Incident.

4.5 **Reporting.** Contractor will provide City of Tukwila with a final written incident report within five business days after resolution of a Security Incident or upon determination that the Security Incident cannot be sufficiently resolved.

5. **Confidential Information or Personal Information**

5.1 **Authorized Personnel.** Contractor will require all Authorized Personnel to meet Contractor's obligations under the Agreement with respect to Confidential Information or Personal Information. Contractor will screen and evaluate all Authorized Personnel and will provide appropriate privacy and security training, as set forth above, in order to meet Contractor's obligations under the Agreement. Upon City of Tukwila's written request, Contractor will provide City of Tukwila with a list of Authorized Personnel. Contractor will remain fully responsible for any act, error, or omission of its Authorized Personnel.

5.2 **Handling of Confidential Information or Personal Information.** Contractor will:

a. Keep and maintain all Confidential Information and Personal Information in strict confidence in accordance with the terms of the Agreement

b. Use and disclose Confidential Information and/or Personal Information solely and exclusively for the purpose for which the Confidential Information or Personal Information is provided pursuant to the terms and conditions of the Agreement. Contractor will not disclose Confidential Information or Personal Information to any person other than to Authorized Personnel without City of Tukwila's prior written consent, unless and to the extent required by applicable law, in which case, Contractor will use best efforts to notify City of Tukwila before any such disclosure or as soon thereafter as reasonably possible. In addition, Contractor will not produce any Confidential Information or Personal Information in response to a non-legally binding request for disclosure of such Personal Information.

5.3 **Data and Privacy Protection Laws.** Contractor represents and warrants that its collection, access, use, storage, disposal, and disclosure of Personal Information complies with all applicable federal, state, local and foreign data and privacy protection laws, as well as all other applicable regulations and directives.

6. **Third Party Security**

6.1 Contractor will conduct thorough background checks and due diligence on any third and fourth parties which materially impact Contractor's ability to provide the products and/or Services to City of Tukwila as described in the Agreement.

6.2 Contractor will not outsource any work related to its products or the Services provided to City of Tukwila in countries outside the United States of America, which have not been disclosed in the Agreement or without prior written approval from City of Tukwila Legal and Information Security. If Contractor desires to outsource certain work during the Term of the Agreement, Contractor shall first notify City of Tukwila so that the parties can ensure adequate security protections are in place with respect to the Services provided to City of Tukwila.

60

7. **Payment Cardholder Data**

7.1 If Contractor accesses, collects, processes, uses, stores, transmits, discloses, or disposes of City of Tukwila and/or City of Tukwila customer credit, debit, or other payment cardholder information, Contractor agrees to the following additional requirements:

   a. Contractor, at its sole expense, will comply with the Payment Card Industry Data Security Standard ("PCI DSS"), as may be amended or changed from time to time, including without limitation, any and all payment card industry validation actions (e.g., third party assessments, self-assessments, security vulnerability scans, or any other actions identified by payment card companies for the purpose of validating Contractor's compliance with the PCI DSS).

   b. Contractor will maintain a continuous PCI DSS compliance program. Annually, Contractor agrees to provide evidence of PCI DSS compliance in the form of a Qualified Security Assessor ("QSA") Assessment Certificate, a PCI Report on Compliance ("ROC"), or evidence that Contractor is included on the Visa or MasterCard list of PCI DSS Validated Service Providers.

   c. Contractor will ensure that subcontractors approved by City of Tukwila, in accordance with Section 6.2, comply with and maintain a continuous PCI DSS compliance program if the subcontractor provides any service on behalf of Contractor that falls within PCI DSS scope. The Subcontractor must provide evidence of PCI DSS compliance in the form of a Qualified Security Assessor ("QSA") Assessment Certificate, a PCI Report on Compliance ("ROC"), or evidence that Subcontractor is included on the Visa or MasterCard list of PCI DSS Validated Service Providers.

   d. Contractor will immediately notify City of Tukwila if Contractor is found to be non-compliant with a PCI DSS requirement or if there is any breach of cardholder data impacting City of Tukwila or its customers.

8. **Changes**

   In the event of any change in City of Tukwila's data protection or privacy obligations due to legislative or regulatory actions, industry standards, technology advances, or contractual obligations, Contractor will work in good faith with City of Tukwila to promptly amend this Exhibit accordingly.

62

<u>OpenGov Contract</u>

Contract to be distributed separately at
the April 28, 2025 Meeting

OpenGov

Tukwila Team,

On behalf of the entire OpenGov team, thank you for the opportunity to collaborate with Tukwila as you chart a course toward a more modern, transparent, and fiscally resilient future. It has been a privilege to work alongside your leadership team—including Aaron, Tony, Joel, Adam, and Tami—who have demonstrated clear vision, pragmatism, and a deep commitment to public service.

After several months of collaboration, demos, workshops, and discussions, it's clear that Tukwila is not simply purchasing new software. You are undertaking a long-overdue modernization of your most foundational citywide functions: budgeting and revenue management. And in doing so, you are positioning Tukwila to meet the demands of a growing community, rising public expectations, and evolving internal capacity challenges.

A Pivotal Moment

Tukwila's legacy systems—CentralSquare Finance Enterprise, Eden Payroll, and spreadsheet-based processes—are no longer sustainable. They may have been sufficient in a simpler era, but today they are creating real operational drag, reducing visibility, and draining valuable staff capacity. Manual reconciliation of tax payments, disconnected Excel files, labor-intensive budget roll-ups, and reactive compliance tracking are not just inefficient—they are barriers to strategic planning, revenue optimization, and transparent governance.

The most recent budget cycle made this clear. Finance staff were consumed by repetitive, manual tasks that delayed reporting, caused rework, and ultimately prevented the team from engaging more meaningfully in strategic decision-making. The City's ability to respond to Council and public inquiries was limited by the structure of its data, not its people. Staff capacity, already stretched thin, could not be augmented due to a lack of systems that enable automation and self-service. The burden was clear—and it took a toll.

Moreover, as Tukwila faces inevitable staffing transitions in the years ahead, succession planning has become a top concern. Much of the City's budget and revenue knowledge lives in the heads of a small group of staff or inside fragile Excel files. The risk of institutional knowledge loss is high. OpenGov's

centralized, auditable, and easy-to-train platform helps mitigate this risk by capturing knowledge in systems—not spreadsheets—and giving new staff a platform that is intuitive, reliable, and fully supported.

Addressing the City's Strategic Priorities

OpenGov was built for this exact moment—and this exact mission. Our integrated cloud platform is purpose-built for local government, and is designed to solve the challenges cities like Tukwila face in budgeting, workforce planning, performance tracking, tax collection, and community engagement.

Build Long-Term Financial Sustainability
- Replace disconnected Excel files with a modern, secure platform that scales with the city's needs.
- Automate budget workflows, approvals, and revisions—freeing staff time for strategic initiatives.
- Integrate daily with CentralSquare Finance Enterprise and support dual-code alignment (FE + BARS).
- Forecast revenues and expenditures with accuracy and speed, enabling long-range planning.
- Fully cost workforce planning scenarios (COLAs, step increases, vacancies, union proposals).
- Future-proof labor planning even as the City prepares to replace its Payroll and ERP Systems in the future.

Unlock $1M+ in Immediate Revenue and ROI
- Transition B&O tax collection from paper to online, with full automation and compliance tracking.
- Quantify, track, and collect more than $1M in missed revenue annually—without adding staff.
- Automate delinquency notices, reconciliation, and audit trails.
- Reduce time spent on reconciliation, error correction, and manual processing.
- Provide businesses with a seamless, transparent portal—improving compliance and satisfaction.

Strengthen Transparency and Community Engagement
- Launch an interactive, web-based budget book with real-time data, embedded narratives, and visual reporting.
- Align budget allocations with community priorities through Priority-Based Budgeting and performance metrics.
- Equip Council with dashboards and reports that drive informed policymaking.
- Provide the public with easy access to meaningful, digestible data on how funds are used and what outcomes are delivered.
- Rebuild trust and engagement around budget decisions and city performance.

Create Capacity and Prepare for the Future
- Eliminate the need for manual data collection and Excel-based roll-ups.
- Free up 100–150 hours per budget cycle, redeploying staff toward strategic and value-added tasks.
  - Ensure continuity of knowledge with centralized systems, documentation, and support.

- Reduce burnout and enhance retention by removing administrative burdens from critical staff.
- Provide a clear, scalable path for cross-training, onboarding, and succession planning.

OpenGov was selected by many of the leading jurisdictions throughout the state and country, including **Duvall, WA ; Mount Vernon, WA ; Anacortes, WA ; Puyallup, WA ; Federal Way, WA ; Stevens County, WA ; Chelan County, WA ;** and **Lewis County, WA**.

PROVIDED SOLUTIONS

Year-Round, Full-Featured Public Sector Budgeting
Maximize end-to-end effectiveness for your entire year-round budget and planning cycle, from near-term forecast adjustments to long-range capital initiatives to continuous budget management and strategic initiative engagement.

- **Collaborative, Automated Operating Budgets:** Liberate your budgeting from disparate spreadsheets with a unified process that seamlessly ties spending to desired outcomes
- **Workforce Planning:** Simplify planning for your most complex and important asset — your people – with scenario analysis, advanced calculations, and integrated budget requests
- **Capital Planning:** Forecast long-term capital expenditures, manage proposals and evaluations, track performance, and easily keep stakeholders from various audiences informed of progress
- **Online Budget Book:** Publish a fully interactive, GFOA award-winning online budget book that makes future publications vastly more repeatable
- **Workflow Management:** Modernize your internal workflows to reduce your administrative burden
- **Reporting & Transparency**: Empower decision makers and the public with the right data in the right format to make data driven decisions and increase public trust.
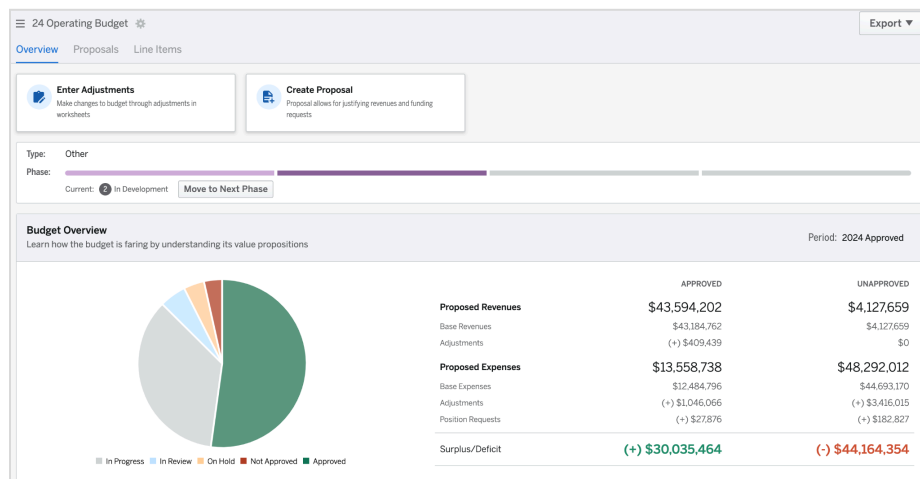
User Home Screen includes At-a-Glance Budget Overview and Tasks

Precisely calculate fully-burdened personnel costs through [workforce planning](#).

Get at-a-glance insights on allocations and the fully-burdened costs of any active or vacant position

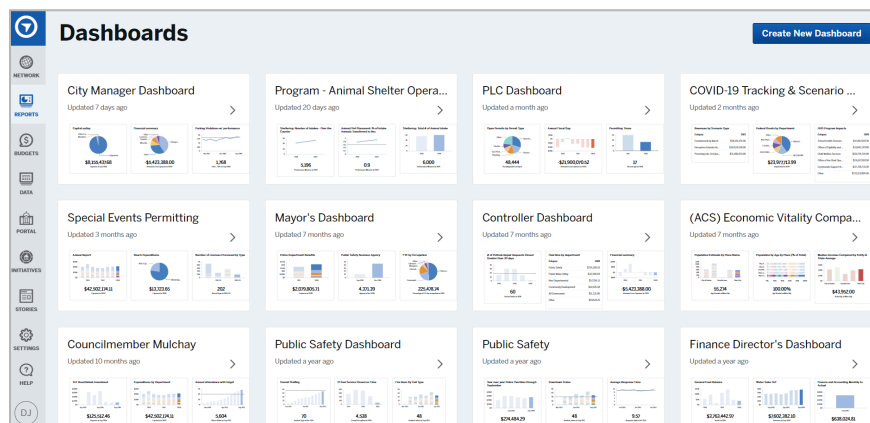**Forecast long-term expenditures for [capital planning initiatives](#).**
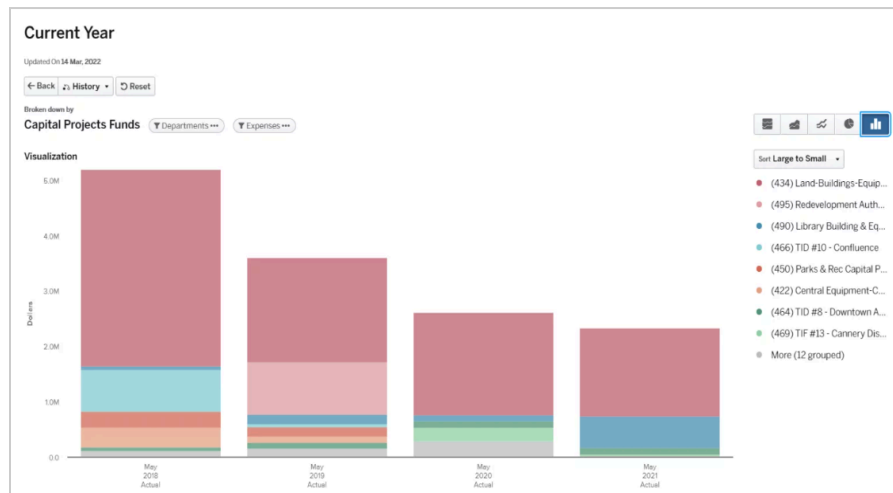
Easy-to-navigate and easy-to-create reports give you insights and drill-downs on your long-term plans

Simplify online budget publications.

Tell Your Story of your Strategic Plan and Budget

Make better decisions with centralized dashboards for everyone.

User Home Screen Includes At-a-Glance Budget Overview and Tasks

Streamline your internal processes

Sample Workflow of a Capital Proposal with Evaluation Details

● Duvall, WA increased their efficiency and streamlined their financial processes – Video

● Santa Cruz County, CA saved over 500 hours during the budgeting process and won a GFOA Distinguished Budget Award – Video

● Vestavia Hills, AL produced their Budget Book 3x faster and had more accurate workforce planning – Case Study

● Alameda, CA cut budget development by 50% and received a GFOA Distinguished Budget Award – Case Study

● Dallas County has modernized its internal budget processes to deliver outcomes for the county– Video

Additional OpenGov Budget + CentralSquare ERP Customers

● City of Torrington, CT

● City of Prescott, AZ

● Township of Cheltenham, Montgomery County, PA

● City of Rancho Cordova, CA

● County of Tuolumne, CA

● City of Foster City, CA

● City of Beaumont, TX

● County of Lewis and Clark, MT

● County of Walton, FL

Key Decision Criteria

Key Considerations for Selecting Tukwila's Long-Term Budgeting & Financial Management Solution

As the City of Tukwila approaches a critical modernization of its budgeting and financial infrastructure, the

importance of selecting a solution that delivers long-term value, operational sustainability, and measurable outcomes cannot be overstated. This decision is not simply about replacing legacy tools—it's about setting the City up for future success, resilience, and transparency. The following considerations are essential as the Council evaluates this strategic investment:

Avoid Low-Cost, Low-Value Software Solutions

Budgeting and financial management require more than surface-level functionality. Solutions marketed as "lightweight" or "cost-effective" often leave cities dependent on external spreadsheets, offer shallow reporting features, and struggle to scale with complexity.

By contrast, OpenGov's Budgeting & Planning Suite was built for the public sector and delivers:
- A centralized environment that replaces brittle Excel files and manual processes
- Automated digital publishing of budget books and capital plans
- No reliance on third-party plug-ins or hidden support fees

The result: organizations that prioritize short-term savings often find themselves re-entering the market within a few years. Tukwila deserves a partner that delivers enduring value.

Real-Time Data Sync with CentralSquare & Eden

Budgeting and reporting must be grounded in data integrity. OpenGov offers automated nightly synchronization with CentralSquare Finance Enterprise and Tyler Eden payroll, ensuring:
- Live updates to budget-to-actuals and transaction records
Real-time data modeling during internal meetings and budget presentations
Confidence in reporting accuracy for both internal stakeholders and Council.

Other vendors may require manual exports or impose update lags—costing time, accuracy, and trust.

Strengthen Capacity and Ensure Continuity of Service

Tukwila's reliance on spreadsheet-driven processes creates serious risks—especially in the event of staff turnover. One of the clearest takeaways from the City's last budget cycle was the fragility of the current approach.

OpenGov directly addresses succession planning and institutional knowledge transfer by providing:
- Centralized, cloud-based data access
- Configurable approval workflows and reporting templates

- Department-facing tools to reduce Finance's manual workload

This ensures continuity and builds operational resilience regardless of staffing changes.

Fully Integrated Capital Planning, Performance & Strategic Goal Alignment

The City's next financial system must support more than just budget development. OpenGov natively supports:
- Six-year Capital Improvement Plans with phase tracking and funding source transparency
- Department-level strategic initiatives tied to budget proposals
- Performance dashboards aligned to program outcomes
- Narrative-based justifications integrated into the public budget book

All of this functionality is built into the OpenGov platform—no separate software, no extra modules.

Transparency, Community Engagement, and Public Trust

Today's residents expect modern digital access to public information. Static PDFs no longer suffice.

OpenGov enables:
ADA-compliant, web-based interactive budget books
Real-time budget visualizations, outcomes tracking, and fund-level insights
Open Town Hall functionality for public surveys, simulations, and input gathering

This is more than just good government—it is critical to sustaining civic trust.

Robust, Forward-Looking Functionality for Long-Term Financial Sustainability

Tukwila's investment must support both the current biennial budget structure and future scenario planning. OpenGov delivers:
- Ten-year forecasting for workforce planning.
- Side-by-side scenario modeling for COLAs, new hires, and union negotiations.
- Visualization of historicals, non-financial data, and GIS-based capital tracking.
- A native report builder that auto-generates reports for Council and the public.
- Built-in publishing tools that meet GFOA standards and ADA compliance.

These capabilities are not theoretical—OpenGov has implemented them in hundreds of jurisdictions.

Built for Washington Municipalities

OpenGov is the selected partner for Duvall, Mount Vernon, Anacortes, Puyallup, Federal Way, Stevens County, Chelan County, and others. Our team understands Washington's requirements, the nuances of CentralSquare, and the state's budgeting and compliance environment.

Our staff includes former City Managers, Finance Directors, and Budget Officers who have been on your side of the table. We don't just understand the technology—we understand the mission.

Why This Matters Now

Tukwila is at a strategic crossroads. The City's current systems lack the depth, resilience, and transparency needed to support modern governance. This is about:

- Expanding staff capacity through automation
- Delivering better, faster data to Council and residents
- Recovering $1M+ in uncollected taxes with improved enforcement
- Supporting program-based budgeting and performance
- Ensuring financial sustainability and data integrity

OpenGov is the only solution on the market that delivers this complete package—with fixed pricing, proven implementation timelines, and a commitment to long-term partnership.

Let's equip Tukwila for the decade ahead.

Competitive Analysis: City of Watsonville, CA RFP

OpenGov was recently evaluated by the City of Watsonville, CA, through a competitive RFP process. The City sought a new solution to replace their manual, Excel-based budget process and address core user needs that were not supported by their Tyler Munis budget module. Despite OpenGov having a higher priced proposal than two other software vendors, the City ultimately decided on moving forward with OpenGov due to the following reasons (we are happy to provide you with a copy of the Council Resolution for more details, if interested):

★ "OpenGov is liked by their customers who appreciate their customer service and the continuous improvements to their product."
★ OpenGov will "allow the Finance Department to move the Capital Improvement Plan (CIP) into the budget system."
★ "OpenGov will automate the creation of the budget book and move the budget book from a published document to an online easily navigable document."

> ★ "OpenGov will save significant finance and communications staff time along with giving departments much more control and transparency around their budget submissions."
>
> ★ "In addition to improving our existing internal processes OpenGov offers a number of features that will enhance our current process particularly around external communication with the public."

Competitive Analysis: City of Oxnard, CA RFP

OpenGov was recently evaluated by the City of Oxnard, CA, through a competitive RFP process. The City also sought a new solution to replace their manual, Excel-based budget process and address core user needs that were not supported by their Tyler Munis budget module. Despite OpenGov having a higher priced proposal than two other software vendors, the City ultimately decided on moving forward with OpenGov due to the following reasons (we are happy to provide you with a copy of the Council Resolution for more details, if interested):

★ City staff received exceptional references from other California cities that use the combination of Tyler Munis and OpenGov, who have leveraged OpenGov's ability to interface with Tyler Munis. Other cities using OpenGov, integrated with Tyler Munis include Hayward, Santa Barbara, Pasadena, Yorba Linda and Victorville.

★ OpenGov offers full-featured, cloud-based, budgeting software designed for public agencies. As an integrated budgeting and planning solution, it will allow staff to develop their department budgets in a more streamlined, systematic, and repeatable way.

Partnership Investment Summary

OpenGov's pricing model consists of both a fixed fee annual subscription for the software and a one-time cost for the professional services component. Our Professional Services cost includes all phases of implementation: Initiation, Best Practices, Configuration, Validation, Deployment, and Project Completion. **OpenGov offers an unlimited user, unlimited usage pricing model, meaning customers are not limited to the number of users, logins, dashboards, reports or usage of data.**

Proposal: OpenGov Budgeting & Performance and Tax Collection & Revenue Management (Full Suite)

Item	Description	3 Year Agreement
Software Services		
Budgeting & Planning Suite Unlimited Users	Operating Budget Workforce Budget Capital Budgeting Capital Project Pages Operating Budget Book Capital Budget Book Nightly Integration – Tyler Munis	
Business Tax and Revenue Management Suite Unlimited Users	Business & Operational Tax Miscellaneous Revenue	**$143,500** *Includes 25% Bundled Discount*
Reporting & Transparency Unlimited Users	Management Reporting Department Reporting Strategic Plan Dashboards, Performance, KPI's Stories Community Feedback Surveys Transparency Portal Strategic Initiatives	
Professional Services		
Software Implementation	Initiation, Best Practices, Configuration, Validation, Deployment, and Project Completion of the above solutions (this includes a review and functional build of your Chart of Accounts into OpenGov).	**~$116,860***
Post-Deployment Training & Support		
Premium Support	Access to phone and chat support, designated Customer Success Manager, and increased response times for support cases.	**Included**
OpenGov University (Unlimited Users)	**OGU On-Demand**: Video-based online learning courses **OGU Live**: a combination of virtual training sessions and in-person	**Included**

	training events* **Resource Center**: a written article knowledgebase	
Customer Success Manager	Dedicated human resource to support your journey as an OpenGov user with training, adoption, best practices, and general assistance throughout the OpenGov partnership	**Included**
Billing Table**		**3Y Agreement**
Year 1		**$260,360**
Year 2		**$150,675**
Year 3		**$158,208**

Estimate – Final Proposal Requires Scoping w/ OpenGov Professional Services Team
**Additional 7.5% Discount Available if Multiple Years Paid Up-Front

Why OpenGov for Tukwila: Budgeting & Planning + Tax & Revenue

As Tukwila takes the next step toward modernizing its financial operations, OpenGov stands uniquely positioned to deliver on the City's most pressing strategic priorities—including fiscal sustainability, transparency, and long-term operational resilience. After months of collaboration with the City's Finance, IT, and executive leadership teams, the following key differentiators explain why OpenGov is the right long-term partner.

Comprehensive, End-to-End Budgeting—Purpose-Built for Government

OpenGov is the only vendor offering a truly unified public sector budgeting solution that covers every stage of Tukwila's annual and biennial planning process in one system:

● Operating Budgeting: Collaborative, department-led budget development with controlled workflows and real-time tracking.

74

● Workforce Budgeting: Powerful salary and benefit modeling with union/step increases, COLA scenarios, and 10-year projections.

● Capital Planning: Project evaluation, proposal scoring, funding source tracking, and auto-generated 6-Year CIP Books.

● Strategic Budgeting: Department requests can be directly tied to citywide initiatives, enabling alignment with Priority-Based Budgeting.

● Public Transparency: Fully interactive, GFOA-compliant online budget books—no third-party publishing tools needed.

● Real-Time Data Sync: Automated nightly integration with CentralSquare FE and structured imports from Eden payroll ensure financial data stays up to date.

Unlike alternatives that rely on third-party plug-ins, external report writers, or disconnected systems, OpenGov eliminates manual uploads and offers seamless, real-time insight—all within a single platform.

Why OpenGov for Tax & Revenue: Intelligent, Automated B&O Management

Tukwila has an estimated $1M/year in uncollected B&O revenue due to limited visibility, lack of automation, and a paper-based returns process. OpenGov's Tax & Revenue platform changes that immediately:

● Modern Taxpayer Portal: Online filings, payments, historical lookup, and multi-user access for third-party preparers.

● Automated Reconciliation: Daily payment and return tracking mapped to the GL with no need for manual line-by-line Excel reconciliation.

● Custom Tax Logic: Supports Tukwila's tiered 9-10-10 penalties, proposed square footage tax, and multiple filing frequencies per account.

● Integrated Case Management: Track audits, assign investigators, and manage compliance workflows with full visibility.

● Proactive Enforcement Auto-generated missing/delinquent notices, account indicators, and configurable templates ensure timely collections.

With OpenGov, Tukwila can replace outdated processes with a professional-grade system that improves compliance, increases revenue, and restores taxpayer confidence.

Solving for Capacity Challenges and Succession Risk

OpenGov reduces reliance on institutional knowledge and eliminates fragile Excel-based workflows. With structured templates, role-based access, and full audit trails, the City can:

● Build capacity across departments by decentralizing input and empowering users.

- Protect against knowledge loss when key staff depart or retire.
- Reduce the volume of one-off support requests into Finance by 30–50%.

This system allows the City to scale effectively and build operational resilience regardless of future staffing changes.

Transparency and Community Engagement—Modernized

OpenGov goes far beyond static PDFs. The platform includes:

- ADA-compliant digital budget books that integrate with performance data and charts.
- Resident engagement tools including survey modules and participatory budgeting (Open Town Hall).
- Council and executive dashboards with on-demand filters, snapshots, and multi-year projections.

Tukwila's Council, executive team, and residents will all benefit from the ability to see where dollars go—and what outcomes they generate.

Lessons from the Last Budget Cycle

The City's most recent budget process highlighted the inefficiencies of Excel-based budgeting:

- Manual version control and formula errors delayed analysis and collaboration.
- Limited ability to model workforce costs by program or department.
- Budget updates during Council presentations could not be modeled live.

OpenGov eliminates these limitations by providing structured, real-time, cloud-based collaboration from the first draft to final adoption.

Demonstrated ROI—Across Budgeting & Revenue

The financial impact of adopting OpenGov is both immediate and ongoing:

- $1M+ in Recaptured Revenue**: Improved tax administration will generate new General Fund revenue.
- 100–150+ Hours Saved Per Budget Cycle**: Staff can focus on strategic planning, not version tracking.
- Increased Compliance**: Automated reminders and digital filing reduce delinquency rates.
- Council & Resident Confidence**: Public-facing transparency strengthens trust and accountability.

Over a 3-year window, these returns significantly outweigh system costs and reduce pressure on city staffing.

Committed to Tukwila's Long-Term Fiscal Sustainability

OpenGov supports multi-year forecasting, 6-year CIP development, and strategic initiative tracking—all key elements of a sustainable financial future. With automated reporting, scenario modeling, and personnel cost forecasting, the City can:

- Align budget decisions with long-term priorities.
- Prepare for labor negotiations and new program needs.
- Surface risks and opportunities early—before budget adoption.

Trusted by Governments Across Washington

OpenGov is already the budgeting and transparency partner of choice for:

Duvall, WA
Mount Vernon, WA
Anacortes, WA
Puyallup, WA
Federal Way, WA
Chelan County, WA
Stevens County, WA

These agencies trust OpenGov for our product expertise, regional knowledge, and local government DNA.

Conclusion

Tukwila deserves a system built for the work of local government—not just another software vendor. OpenGov offers an integrated platform to unify budgeting and revenue management, elevate public trust, and ensure the City's financial sustainability for years to come.

Our team of former public finance leaders, technologists, and customer success experts is ready to support Tukwila through every step of implementation, adoption, and continuous improvement.

Let's build the next chapter of Tukwila's future—together.