

Addendum # 1
Daytime, After-Hours and Continuity of Service Dispatch Services
Job # RFP 29-23-PW

Note to all Respondents:

The length of the contract for the dispatch services will be for a period of three years with one two-year extension upon mutual agreement of the City and vendor.

Proposers shall include a signed IT Cloud Vendor Security Agreement and Non-Disclosure Agreement with their proposals. These documents are listed both at the end of this document, and can also be found as an attachment on the City's website that can be found here:

<https://www.kirklandwa.gov/Government/Departments/Finance-and-Administration/Purchasing-Services/Doing-Business-with-the-City>

Responses to RFP Questions

1. Please reconfirm the due date for this procurement by providing it in response to answers to questions.

Please see RFP, page 2 for submittal instructions. All proposals are due by 4:00 PM Pacific Time on Monday, July 24, 2023.

2. Are bidders permitted to deviate in any way from any manner of quoting fees you may be expecting? For example, if there is a pricing page in the RFP, can bidders submit an alternate fee structure? If there is no pricing page in the RFP, do you have any preference for how bidders should quote fees or can bidders create their own pricing categories?

Please see RFP, page 7, Rate and Service Structure and page 12, Compensation. City does not have a preference for how bidders quote fees. However, the fee structure submitted must be comprehensive so the City can accurately project all fees for the service that would be charged.

3. Please describe your level of satisfaction with your current or recent vendor(s) for the same purchasing activity, if applicable.

We are satisfied with the current vendor.

4. If this is a term contract subject to renewal, what is the term and the maximum number of option periods?

The length of the contract for the dispatch services will be for a period of three years with one two-year extension upon mutual agreement of the City and vendor.

5. Has the current contract gone full term?

No, the current contract expires September 30, 2023.

6. Have all options to extend the current contract been exercised?

Yes, options to extend the contract have been exercised.

7. Who is the incumbent, and how long has the incumbent been providing the requested services?

The incumbent is Daupler and we have had a contract with them for just over a year.

8. To what extent will the location of the bidder's proposed location or headquarters have a bearing on any award?

Please see RFP, Scope of Services, section 10.

9. How are fees currently being billed by any incumbent(s), by category, and at what rates?

The 12-month pilot contract cost was \$6,000 plus an additional \$2,900 to extend for three months thereafter.

10. What estimated or actual dollars were paid last year, last month, or last quarter to any incumbent(s)?

The 12-month pilot contract cost was \$6,000, paid in full last year. In June of 2023, we paid an additional \$2,900 to extend the contract for three months.

11. Is previous experience with any specific customer information systems, phone systems, or software required?

No, previous experience is not required but is preferred.

12. What is the minimum required total call capacity?

Please see RFP, Introduction.

13. What is the minimum simultaneous inbound call capacity?

Please see RFP, Scope of Services, section 5.

14. What is the maximum wait time?

Please see RFP, Scope of Services, section 4 for more information; maximum wait time is not specified but an alternate greeting should be offered while on hold. We would hope that sufficient staff will be hired and trained to assure that the City's service requirements are met.

15. What is the maximum hold time?

Please see RFP, Scope of Services, section 4 for more information; maximum wait time is not specified but an alternate greeting should be offered while on hold. We would hope that sufficient staff will be hired and trained to assure that the City's service requirements are met.

16. What percentage of inbound calls must be answered by a live operator?

Please see RFP, Scope of Services, section 7 for more information.

17. What percentage of calls must be resolved without a transfer, second call, or a return call?

This information is not specified by the City but customer service is a high priority for the City.

18. What is the maximum percentage of calls that can be terminated by the caller without resolution?

This information is not specified by the City but customer service is a high priority for the City.

19. Is there a minimum or maximum number of operators and supervisors?

This information is not specified by the City of Kirkland but customer service is a high priority for the City and calls must be answered by the third ring. Please see RFP, Scope of Services, section 10.

20. What is the required degree of dedication for the operators? (Can operators work on other contracts at the same time as this one)?

Please see RFP, Scope of Services. Customer service is a high priority for the City.

21. What are the recording requirements for inbound and outbound phone calls and how long must recordings be maintained?

Please see RFP, Scope of Services, section 12. The audio of the phone calls is not required to be recorded, but a log must be maintained.

22. What are the recording and storage requirements for non-phone communications?

Please see RFP, Scope of Services, section 12.

23. What is the current number of seats for operators and supervisors at your existing call center?

This information is not available.

24. What is the current average wait time for phone calls?

This information is not available.

25. What is the current average handle time for phone calls and other types of communications?

This information is not available.

26. What is the current average after-call work time for operators?

This information is not available.

27. Over the past year, what is the percentage of calls received in English versus non-English?

This information is not available.

28. Over the past year, what percentage of calls received were in Spanish?

This information is not available.

29. What time of day, days of the week, or times of the year do calls typically peak?

Most calls generally occur weekdays between 9am to 3pm. Call volumes peak during inclement weather.

30. Whether companies from Outside USA can apply for this? (like, from India or Canada)

Please see RFP, Scope of Services, section 10.

31. Whether we need to come over there for meetings?

Please see RFP, Scope of Services, section 10.

32. Can we perform the tasks (related to RFP) outside USA? (like, from India or Canada)

Please see RFP, Scope of Services, section 10.

33. Can we submit the proposals via email?

Please see RFP, Proposal Submittal Instructions.

34. Would proof of insurance meeting the requirements detailed in the RFP and a copy of a City of Kirkland business license be required as part of our RFP proposal?

Please see RFP, Contracting Requirements and Fees.

35. What is the current budget for operating this contact center?

There isn't a budget allocated at this time.

36. Does the agency have an existing knowledge repository that the vendor will use for its agents?

The City can provide service area maps, a list of issues and whether they should trigger dispatch to on-call personnel or not as well as other assistance as needed.

37. Will the City consider providing the selected vendor direct access to Lucity to create and manage service requests?

Vendor will not have direct access to Lucity. Please see RFP, Scope of Service, section 2.

38. Are the agent workflow or training materials provided?

The City can provide service area maps, a list of issues and whether they should trigger dispatch to on-call personnel or not as well as other assistance as needed.

39. What is the City's length of training for call workflows, knowledge and any systems?

This will be a joint effort with the vendor after workflows are jointly determined. Length of training is unknown at this time but probably not to exceed one month.

40. Please advise if the 1,500-3,000 calls annually for these services are for daytime, after-hours and holidays or solely after-hours and holidays?

The number of calls is an estimate of total calls annually. We receive an average of 50 calls per month after-hours.

41. Is the City solely seeking a vendor for after-hours operations and inclement weather when City buildings are closed or are you seeking a vendor for daytime operations as well?

The City is seeking a vendor for daytime operations as well.

42. What is the current average speed of answer (ASA) and your goal for the new vendor?

This information is not available.

43. Does the city currently send mass notifications via text to impacted customers during emergencies and planned maintenance projects?

No, the City does not currently send mass notifications.

44. What are your key challenges and opportunities?

The City would like to relieve on-call personnel from having to assemble a crew after-hours for responding to an emergency, inform callers preemptively regarding outages, update callers with real-time information during an emergency, and allow callers to interact with vendor software in order to submit additional information and pictures.

45. What are the critical success factors for a new vendor?

Please see RFP. City but customer service is a high priority for the City.

46. The title and Introduction of the RFP references daytime dispatch services. The Scope of Services does not make any indication of daytime usage. Should the vendor be prepared to provide services 24/7, 365 days? Additionally, is the estimated call volume of 1,500-3,000 inclusive of daytime calls?

The vendor should have the capability to provide services 24/7, 365 days. Yes, the estimated call volume includes daytime calls.

47. In reference to the functionality described in Scope of Services, section 6, is it required that this is performed by software? Should the “call groups” be set up in a way that allows the City to callout by multiple categories, including titles, roles, and skillsets?

Yes, functionality described in Scope of Services, section 6, should be performed by software. Software should allow call groups to be set up by titles, roles and skill sets.

48. In reference to Scope of Services, section 18, is it required that this is performed by software? Are these messages intended to be sent both reactively (after a person calls in) and proactively (by the City before a person calls in)?

Yes, Scope of Services, section 18, is required to be performed by software both reactively and proactively.

49. In reference to Scope of Services, section 3, is it required that the on-call crew member acknowledge the notification? If so, is it required that the acknowledgement take place in software for documentation purposes?

Yes, Scope of Services, section 3, requires that the on-call crew member acknowledge the notification. And that the acknowledgement take place using the software.

50. In reference to Scope of Services, section 3, if the initial on-call personnel doesn't acknowledge receipt of the information, should additional personnel be contacted? If so, is it required that this process take place via software?

Yes, if the initial on-call personnel doesn't acknowledge receipt of the information, additional personnel should be contacted per protocol provided by City and this is required to be documented in the software.

51. In reference to Scope of Services, section 4, is the referenced “recording indicating that we are aware of the situation” required? If so, is it required for the vendor to have the ability to identify and trigger this on behalf of the City?

Vendor's ability to implement reactive messaging during emergencies would be helpful and avoid hold time for customers.

52. Are there any other sources of information that you would require the vendor to monitor, such as utility locates, alarms, sensors, etc.?

Scope of Services, section 11, describes the types of calls the vendor will receive. Vendor should be able to monitor telemetry alarms and sensors in the future if needed.

53. Is it required that the awarded vendor enable the on-call personnel to contact the reporting party without revealing the on-call personnel's phone number?

Yes, hiding the on-call personnel's phone number when calling the customer is required.

54. In reference to Scope of Services, section 19, is it required that this is completed by software?

No, however, efficiently accomplishing this likely will require software.

IT Cloud Vendor Security Agreement

This IT Cloud Vendor Security Agreement (“Security Agreement”) is entered into by and between the City of Kirkland, (“City”), and _____ (“Vendor”)

Scope: This policy applies to all Vendors who do any form of work (“Contract”) with the City of Kirkland that includes possession, storage, processing, or transmission of Personally Identifiable Information (PII), Sensitive Personal Information (SPI) or Personal Health Information (PHI) for City of Kirkland employees, volunteers, contractors, and/or citizens in any location that is outside of the City of Kirkland Firewalls. This includes public and private cloud infrastructures and Vendor’s own infrastructure on their premises. This is regardless of who the Vendor is and which department they are working for or with, and it applies to all locations where the Vendor stores information.

If this Contract covers only PII or SPI, then only this addendum must be signed.

If this Contract covers PHI, then this addendum must be signed, and a HIPAA Business Associates Agreement must also be signed and incorporated as an addendum to this document or as an addendum to the Contract.

This policy does NOT apply to CJIS data (criminal justice data). There is a separate federally mandated addendum that covers protection of CJIS data, which must also be signed if the Contract includes such information.

Provision: When possible, this policy should be an addendum to existing contracts with vendors. It may be signed separately when necessary.

Duration: This policy applies from the time a vendor signs its Contract with the City through such point in time that all data which was in the vendor’s control is returned to the City and destroyed at the City’s request, including but not limited to backups, test sites, and disaster recovery sites.

Definitions:

Personally Identifiable Information (PII), or Sensitive Personal Information (SPI):

Information that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

Protected Health Information (PHI): any information about health status, provision of health care, or payment for health care that can be linked to a specific individual, which is more particularly defined under HIPAA (Title 45, CFR) and the Health Care Information Act (RCW Chapter 70.02).

Vendor: Includes owners and employees, volunteers, subsidiaries, and any subcontractors who might reasonably have access to this data.

Options:

Option 1: A vendor can verify that they have a high level of security certification that is satisfactory to the City of Kirkland. Examples include but may not be limited to SOC2 and FedRamp.

If this option is selected, print the mutually agreed upon certification level below and attach appropriate documentation.

Option 2: Vendors can agree to follow the following security best practices:

1. All customer data will be stored on servers physically located in the United States.
2. All customer data will be stored in a location with reasonable physical controls where data will not be visible to anyone not covered by this policy.
3. Access to data will only be provided on a need to know basis in order for the vendor to complete this work.
4. Data will not be shared with an outside third party without explicit written consent of the City.
5. Data will be encrypted prior to and during any transfer from one location to another.
6. Data will be disposed of appropriately, including shredding or burning of any printed versions and destruction or secure erasure of any electronic medium on which data has been stored.
7. Vendor agrees to the appropriate internal certification for vendor staff who access the data (for example, PHI must only be handled by vendors who have HIPPA training).
8. Vendor staff with access to City of Kirkland data covered by this policy must pass a criminal background check prior to accessing that data.
9. Vendors must perform internal and/or external security auditing on a regular basis that is no less common than once per year.
10. Vendors shall abide by the following policies for passwords:
 - a. Network login passwords must be at least 8 characters long and include at least one number and one capital letter.
 - b. Passwords must be changed every 90 days.
 - c. The same password cannot be re-used within twenty password changes.
 - d. Passwords must not be written down or stored in systems except in encrypted applications designed to store passwords.
 - e. Passwords must not be shared among vendor staff.
 - f. Vendors should not use the same passwords for City and personal needs.
 - g. Other password protected systems will comply with above network login password policy when technically possible.
11. Vendors must report all security incidents to the appropriate City of Kirkland IT personnel, including any serious security breaches on their own network, within 24 hours of identifying the security incident.
12. In the event of a data breach, Vendor must have an internal policy to provide for timely forensic investigation of affected and related servers and must follow all state, local, and federal requirements for notifying individual's whose PII or PHI has been or may have been breached.

13. Vendor's servers must be patched on a regular and timely basis with all security-related patches from application and infrastructure vendors.
14. Data must be kept in at least two different physical locations. One location can be in a compressed format (e.g., as a backup file).
15. Vendor must enable logging as follows:
 - a. Logs are enabled for common third-party applications
 - b. Logs are active by default
 - c. Logs are available for review by the City of Kirkland for up to one year
 - d. Logs are retained for up to one year

Any deviation from the above best practices must be described here and mutually agreed upon (Signatures on this policy will constitute mutual agreement).

Description of any area where vendor is requesting a waiver, an agreement to a different method, or any other change to this policy:

A breach of this Security Agreement also constitutes a breach of any agreement to which it is appended and the City may terminate either or both because of such breach as soon as it must to mitigate that breach or others that may then be apparently forthcoming. The City agrees to work with the Vendor to avoid such termination if reasonably possible but protection of the information held by the Vendor cannot be compromised in the process.

Description of data in the Vendor's care (attach additional sheets if necessary):

Is this an addendum to an existing or new contract (Y/N): ____

If yes, name and duration of contract: _____

City business person responsible for contract and vendor management:

| | | |
|------|-------|------------|
| Name | Title | Department |
|------|-------|------------|

City IT person responsible for contract and vendor management:

| | | |
|------|-------|------------|
| Name | Title | Department |
|------|-------|------------|

The following signature block must be completed. By signing this agreement, vendor warrants that they are responsible for the security of the PII, SPI, and/or PHI in their care.

| |
|-----------------------|
| VENDOR NAME. |
| _____ Signature |
| _____ Printed Name |
| _____ Title |
| _____ Date |

| |
|-----------------------|
| City of Kirkland |
| _____ Signature |
| _____ Printed Name |
| _____ Title |
| _____ Date |



NON-DISCLOSURE AGREEMENT

This Non-Disclosure Agreement (“the Agreement”) is made this _____ day of _____, 202____, by and between the City of Kirkland, a municipal corporation of the State of Washington (the “City”), and _____, a ___ <Corporation/partnership/limited liability company, etc.> (“the Vendor”).

Whereas, the Vendor <is the successful candidate/wishes to submit a proposal>for the <project name>; and

Whereas, the Vendor will need to review confidential information (“Confidential Information¹”) belonging to the City in order to be able to <prepare its proposal/complete this project>, which the City does not want disclosed; and

Whereas, in consideration for being allowed to see the Confidential Information so that it can <prepare a proposal or complete the project>, the sufficiency of such consideration being hereby acknowledged, the Vendor is willing to enter into this Non-Disclosure Agreement.

Now, therefore, as evidenced by their signatures below, the parties hereby agree as follows:

1. The Vendor shall maintain and protect the confidentiality of the Confidential Information, shall not disclose the Confidential Information to any person or entity, and shall not challenge, infringe or permit or assist any other person or entity to disclose the Confidential Information or challenge or infringe any of the City’s license rights, trade secrets, copyrights, trademarks or other rights respecting the Confidential Information.
2. Except pursuant to a written agreement between the parties, the Vendor shall not directly or indirectly, i) provide, make, use or sell, or permit or assist any other person or entity to provide, make, use or sell any services, devices or products incorporating any protected feature embodied in any of the Confidential Information; ii) apply for or seek to register, or otherwise attempt to create, establish or protect any patents, copyrights or trademarks with respect to any of the Confidential Information; or iii) use any name used by the other party, whether or not subject to trademark protection, or any confusingly similar name.
3. The Vendor shall not disclose the Confidential Information except to those persons employed by the Vendor, or its affiliates or subsidiaries, who have reasonable need to review the Confidential Information under the terms of this Agreement who have agreed to be bound the terms of this Agreement or a similar agreement that is at least as protective of the Confidential Information as provided for herein.
4. Vendor shall not make any copies, drawings, diagrams, facsimiles, photographs or other representations of any of the Confidential Information.

¹ “Confidential Information” means the information the City has provided the Vendor by or at the direction of the City, or to which access was provided to the Vendor by or at the direction of the City, in the course of the Vendor’s wish to submit a proposal or complete this project.

5. Upon request by the City, Vendor shall immediately destroy or return any Confidential Information in its possession, including all copies thereof.
6. Notwithstanding other provisions of this Agreement, the Agreement does not restrict the Vendor with respect to the use of information that is already legally in its possession, that is available to the Vendor from other sources without violating this Agreement or the intellectual property rights of the City, or that is in the public domain. Notwithstanding other provisions of this Agreement, this Agreement also shall not restrict the Vendor from providing, making, using or selling services, devices or other products so long as the Vendor does not breach this Agreement, violate the City's intellectual property rights or utilize any of the Confidential Information.
7. The Vendor, its officers, agents and employees, agrees to hold harmless, indemnify and defend at its own expense the City, its officers, agents and employees, from and against any and all claims of any kind whatsoever arising out of the Vendor's intentional acts or negligent failure to perform any of its obligations under this Agreement.
8. The covenants in this Agreement may be enforced a) by temporary, preliminary or permanent injunction without the necessity of a bond or b) by specific performance of this Agreement. Such relief shall be in addition to and not in place of any other remedies, including but not limited to damages.
9. In the event of a suit or other action to enforce this Agreement, the substantially prevailing party shall be entitled to reasonable attorneys' fees and the expenses of litigation, including attorneys' fees, and expenses incurred to enforce this Agreement on any appeal.
10. The Agreement shall be governed by and construed in accordance with Washington law. The King County Superior Court or the United States District Court for the Western District of Washington at Seattle (if federal law is applicable) shall have the exclusive subject-matter jurisdiction of matters arising under this Agreement, shall have personal jurisdiction over the parties and shall constitute proper venue for any litigation relating to this Agreement.
11. For purposes of this Agreement, all covenants of the Vendor shall likewise bind the officers, directors, employees, agents, and independent contractors of the Vendor, as well as any direct or indirect parent corporation of the Vendor, direct or indirect subsidiary corporations of the Vendor and any other person or entity affiliated with or related to the Vendor or to any of the foregoing persons or entities. The Vendor shall be liable to the City for conduct of any of the foregoing persons or entities in violation of this Agreement to the same extent as if said conduct were by the Vendor.
12. The Vendor shall not directly or indirectly permit or assist any person or entity to take any action which the Vendor would be barred by this Agreement from taking directly.
13. This Agreement shall bind and inure to the benefit of the heirs, successors and assigns of the parties.

IN WITNESS WHEREOF, the parties have duly executed this Agreement on the day and year first written above.

CITY OF KIRKLAND

<Company Name>

By:_____

By:_____

Its:_____

Its:_____