REQUEST FOR QUOTATIONS

Title: **Emergency Notification System (ENS)**

Reference No.: 1220-040-2019-095

FOR THE ACQUISITION OF SOFTWARE AS A SERVICE INFORMATION TECHNOLOGY SOLUTIONS

(General Services)

Issue Date: November 7, 2019

TABLE OF CONTENTS

REQUEST FOR QUOTATIONS

1. INTRODUCTION

1.1 Purpose

The City of Surrey (the "**City**") invites Contractors to provide quotations for an emergency notification system (the "**Emergency Notification System**" or "**ENS**") to support the City's emergency response needs. The purpose of this request for quotations (the "**RFQ**") is to invite quotations for the supply of an ENS, including software licensing, implementation services, education and training, support and maintenance, and associated software and services, as described in Schedule A to this RFQ (the "**Services**") to be provided on a time and materials basis

1.2 Definitions

In this RFQ the following definitions shall apply:

"**BC Bid Website**" means www.bcbid.gov.bc.ca;

"**City**" means the City of Surrey;

"**City Representative**" has the meaning set out in section 2.4;

"**City Website**" means www.surrey.ca;

"**Contract**" means a formal written contract between the City and a Contractor(s) to undertake the Services, the preferred form of which is attached as Schedule B – Attachment 1;

"**Contractor**" has the meaning set out in section 1.2;

"**Information Meeting**" has the meaning set out in section 2.3;

"**Emergency Notification Software**" has the meaning set out in section 1.1;

"**Quotation**" means a quotation submitted in response to this RFQ;

"**RFQ**" means this Request for Quotations; and

"**Services**" has the meaning set out in section 1.1.

1.3 Anticipated Solicitation Schedule

The following is the City's estimated timeline for the project.

Solicitation Schedule	Estimated Dates
Issuance of the RFQ	November 7, 2019
Date (preferred)	November 28, 2019, 4:00pm

Evaluation of Quotations	December 2-6, 2019
Interviews/Demonstrations dates for Preferred Contractors only (if any)	December 9-20, 2019
Finalization of the Contract	January 2020
Expected "Go Live" Date	February 2020

2. DELIVERY OF QUOTATIONS

2.1 Address for Delivery

A Quotation should be labelled with the Contractor's name, RFQ title and number. A Quotation should be submitted in the form attached to this RFQ as Schedule C – Quotation.

The Contractor may submit a Quotation either by email or in a hard copy, as follows:

(a) Email

If the Contractor chooses to submit by email, the Contractor must submit the Quotation electronically in a single pdf file to the City by email at: purchasing@surrey.ca.

PDF emailed Quotations are preferred and the City will confirm receipt of emails. Note that the maximum file size the City can receive is 10Mb. If sending large email attachments, Contractors should phone to confirm receipt. A Contractor bears all risk that computer equipment functions properly so that the City receives the Quotation.

(b) Hard Copy

If the Contractor chooses NOT to submit by email, the Contractor should submit one (1) original unbound Quotation and one (1) copy (two (2) in total) which must be delivered to the City at the office of:

Name: Richard D. Oppelt, Manager, Procurement Services
at the following location:

Address: Surrey City Hall
Finance & Technology Department – Purchasing Section
Reception Counter, 5th Floor West
13450 – 104 Avenue, Surrey, B.C., Canada V3T 1V8

2.2 Date

The City would prefer to receive Quotations on or before November 28, 2019. The City's office hours are 8:30 a.m. to 4:00 p.m., Monday to Friday, except statutory holidays.

2.3 Inquiries

All inquiries related to this RFQ should be directed in writing to the person named below (the "**City Representative**"). Information obtained from any person or source other than the City Representative may not be relied upon.

Name: Richard D. Oppelt, Manager, Procurement Services
Address: 13450 – 104 Avenue, Surrey, British Columbia, V3T 1V8
Fax: 604-599-0956
E-mail: purchasing@surrey.ca
Reference: 1220-040-2019-095

2.4 Addenda

If the City determines that an amendment is required to this RFQ, the City Representative will issue a written addendum by posting it on the BC Bid Website at www.bcbid.gov.bc.ca (the "**BC Bid Website**") and the City Website at www.surrey.ca (the "**City Website**") that will form part of this RFQ. It is the responsibility of Contractors to check the BC Bid Website and the City Website for addenda. The only way this RFQ may be added to, or amended in any way, is by a formal written addendum. No other communication, whether written or oral, from any person will affect or modify the terms of this RFQ or may be relied upon by any Contractor. By delivery of a Quotation, Contractor is deemed to have received, accepted and understood the entire RFQ, including any and all addenda.

2.5 City's Preferred Forms of Contract

The City's preferred forms of contract for the Services are included in this RFQ as Schedule B-1. Contractors should consider all specifications, requirements, terms and conditions of the form of contract applicable to their proposed solution in their Quotations.

A Contractor should not submit its own standard contract terms and conditions as a response to this RFQ. Instead, the Contractor should review and identify the language in the City's attached Contract that the Contractor finds problematic, state the issue, and propose the language or contract modifications Contractor is requesting. The Contractor should keep in mind, when requesting such modifications, that the City is not obligated to accept the requested changes.

The City is not obligated to accept any modifications, but may choose to accept some, none, or all proposed modifications that a Contractor has submitted with its Quotation.

3. QUOTATION FORM AND CONTENTS

3.1 Package Form (Hard Copy)

If the Contractor chooses NOT to submit by email, the City encourages Contractors to submit Quotation packages which support the green expectations and initiatives of the City. Quotations should be in a format that reduces paper usage (double sided printing is encouraged), uses recycled products, and reduces package bulk. Binders, large packages, and vinyl plastic products are unwanted.

3.2 Form of Quotation

Contractors should submit Quotations in the form attached as Schedule C, including Schedules C-1 to C-5. Contractors are encouraged to respond to the items listed in Schedules C-1 to C-5 in the order listed. Contractors are encouraged to use the forms provided and attach additional pages as necessary.

A Quotation should include sufficient information to allow the City to verify the total cost for the project and determine whether the City's requirements for the Services can be met. Quotations should respond to requests for information in the above noted schedules, whether the request requires a simple "yes" or "no" or requires a detailed narrative response.

3.3 Signature

The legal name of the person or firm submitting the Quotation should be inserted in the Quotation. The Quotation should be signed by a person authorized to sign on behalf of the Contractor and include the following:

(a) If the Contractor is a corporation then the full name of the corporation should be included, together with the names of authorized signatories. The Quotation should be executed by all of the authorized signatories or by one or more of them provided that a copy of the corporate resolution authorizing those persons to execute the Quotation on behalf of the corporation is submitted;

(b) If the Contractor is a partnership or joint venture then the name of the partnership or joint venture and the name of each partner or joint venturer should be included, and each partner or joint venturer should sign personally (or, if one or more person(s) have signing authority for the partnership or joint venture, the partnership or joint venture should provide evidence to the satisfaction of the City that the person(s) signing have signing authority for the partnership or joint venture). If a partner or joint venturer is a corporation then such corporation should sign as indicated in subsection (a) above; or

(a) If the Contractor is an individual, including a sole proprietorship, the name of the individual should be included.

3.4 Content of Quotation

Contractors should prepare Quotations to meet the minimum requirements for the Services as set out in this RFQ, but may, at their election, include additional services.

4. REVIEW OF QUOTATIONS

4.1 Review of Quotations

The City will review all received Quotations to determine which Quotation is most advantageous to the City by application of the following evaluation criteria:

(a) Experience, Reputation and Resources
(the review team will consider responses to items in Schedule C-2)

(b) Technical – quality and functionality of the Emergency Notification System (including Functional & Technical Requirements)
(the review team will consider responses to items in Schedule C-3, including Schedule C-3-1 – Functional and Technical Requirements and Schedule C-4 – Contractor's Technical Quotation (Time Schedule))

(c) Financial, including prices (including initial and on-going prices) and financial strength
(the review team will consider responses to Schedule C-5, including Schedule C-5-1)

(d) Modifications requested by Contractor to Contract – including changes to risks to the City and costs
(the review team will consider Contractor's response to Schedule C-1)

The City may compare one Contractor's Quotation to another Contractor's Quotation in its review of Quotations. The City's intent is to acquire the solution for the Services that provides the best value to the City and meets or exceeds both the functional and technical requirements identified in this RFQ.

In applying the evaluation criteria the City will not assign specific weighting to any criteria. The City is not obligated to select the lowest price.

4.2 Discrepancies in Contractor's Financial Quotation

If there are any obvious discrepancies, errors or omissions in Schedule C-5-1 of a Quotation (Contractor's Financial Quotation), then the City shall be entitled to make obvious corrections, but only if, and to the extent, the corrections are apparent from the Quotation as submitted, and in particular:

(a) if there is a discrepancy between a unit price and the extended total, then the unit prices shall be deemed to be correct, and corresponding corrections will be made to the extended totals;

(b) if a unit price has been given but the corresponding extended total has been omitted, then the extended total will be calculated from the unit price and the estimated quantity; and

(c) if an extended total has been given but the corresponding unit price has been omitted, then the unit price will be calculated from the extended total and the estimated quantity.

4.3 Litigation

If the Contractor, or any officer or director of the Contractor, is or has been engaged directly or indirectly in a legal action against the City, its elected or appointed officers, representatives or employees in relation to any matter, or if the City has initiated legal action against any officers or directors of the Contractor, the City may consider such litigation in its review of the Contractor's Quotation under Section 4.1. The City will consider whether such litigation is likely to affect the Contractor's ability to work with the City, and whether the City's experience with the Contractor indicates an increased risk of

the City incurring additional costs in the administration of the Contract and/or carrying out of the Services if the Contract is awarded to the Contractor.

4.4 Additional Information

The City may, at its discretion, request clarifications or additional information from a Contractor with respect to a Quotation, and the City may make such requests to only selected Contractors. The City may consider such clarifications or additional information in its review of a Quotation.

4.5 Interviews/Presentations

The City may, at its discretion, invite some or all of the Contractors to appear before the City to provide clarifications of their Quotations. In such event, the City will be entitled to consider the answers received in its review of Quotations. Contractor management and technical personnel may be requested to participate in presentations, demonstrations and/or interviews.

4.6 Multiple Contractors

The City reserves the right and discretion to divide up the Services, either by scope, geographic area, or other basis as the City may decide, and to select one or more Contractors to enter into discussions with the City for one or more Contracts to perform a portion or portions of the Services. If the City exercises its discretion to divide up the Services, the City will do so reasonably having regard for the RFQ and the basis of Quotations.

In addition to any other provision of this RFQ, Quotations may be reviewed on the basis of advantages and disadvantages to the City that might result or be achieved from the City dividing up the Services and entering into one or more Contracts with one or more Contractors.

5. GENERAL CONDITIONS

5.1 No Contract

A Quotation submitted in response to this RFQ is, when received by the City, an offer to the City to perform the Services on the terms as described in this RFQ. This RFQ is an invitation to the Contractor to prepare and submit a Quotation as an offer. This RFQ is not a tender or a request for proposals and no obligations of any kind will arise from this RFQ or the submission of Quotations. This RFQ does not commit the City in any way to select a Contractor, or to proceed to negotiations for a Contract, or to award any Contract, and the City reserves the complete right to at any time reject all Quotations and to terminate this RFQ process.

5.2 Acceptance

The City may at any time by written notice to a Contractor(s) accept the Contractor's Quotation unless prior to the receipt of such written notice the Contractor has, by written notice to the City, revoked its Quotation. (Following the time for delivery of Quotations as set out in Section 2.3, the City will not accept any amendments to a submitted Quotation.)

The City may negotiate changes to any terms of a submitted Quotation, including negotiation of amendments to a Contractor's prices included in its Quotation, and may negotiate with one or more Contractors.

5.3 Administration of RFQ Process

The City will keep Quotations confidential, and in administering the RFQ process will endeavour to treat all Contractors with fairness and impartiality.

5.4 Contractor's Expenses

Contractors are solely responsible for their own expenses in preparing, and submitting Quotations, and for any meetings, negotiations or discussions with the City or its representatives and consultants, relating to or arising from this RFQ. The City and its representatives, agents, consultants and advisors will not be liable to any Contractor for any claims, whether for costs, expenses, losses or damages, or loss of anticipated profits, or for any other matter whatsoever, incurred by the Contractor in preparing and submitting a Quotation, or participating in negotiations for a Contract, or other activity related to or arising out of this RFQ.

5.5 Contractor's Qualifications

By submitting a Quotation, a Contractor represents that it has the expertise, qualifications, resources and relevant experience to perform the Services.

5.6 Conflict of Interest

A Contractor shall disclose in its Quotation any actual or potential conflicts of interest and existing business relationships it may have with the City, its elected or appointed officials or employees. The City may rely on such disclosure.

5.7 Solicitation of Council Members, City Staff and City Consultants

Contractors and their agents will not contact any member of the City Council, City staff or City consultants with respect to this RFQ, other than the City Representative named in section 2.6, at any time prior to the award of a contract or the cancellation of this RFQ.

5.8 Confidentiality

All submissions become the property of the City and will not be returned to the Contractor. All submissions will be held in confidence by the City unless otherwise required by law. Contractors should be aware the City is a "public body" defined by and subject to the *Freedom of Information and Protection of Privacy Act* of British Columbia.

5.9 City's Right to Accept or Reject Any Quotation or All Quotations

The City reserves the right to accept or reject any Quotation that is not in the preferred format, does not address all the requirements of this RFQ, objects to the terms and conditions of this RFQ, or that the City determines is excessive in price or otherwise not in the City's best interest to accept. In addition, the City may cancel this RFQ, reject all the Quotations, and seek to do the project through a new RFQ or other means.

SCHEDULE A – SCOPE OF SERVICES

EMERGENCY NOTIFICATION SYSTEM (ENS)

1. SCOPE OF SERVICES

The City of Surrey (the "City") is requesting Quotations for an Emergency Notification System (ENS) that will fulfill the requirements as stated in this Scope of Services, including both a system product and the services to implement that product.

The products and services desired include the application, implementation, configuration, testing and training as well as ongoing maintenance and support. If multiple solutions are required, Quotations that require partnerships between Contractors are invited as necessary to meet the City's ENS requirements for an automated system to contact all required parties in the event of an emergency.

An ENS package is a critical communication tool that will further enhance the City's Business Continuity Management Program (BCMP) and striving towards a more resilient organization. This falls under the City's Business Continuity Management Program, Emergency Response Program and Disaster Recovery Program.

Abstract

The BCMP will operate and direct the ENS. The chosen system will provide alerts, notifications, warnings, and other similar operations during all hazards, threats, and emergencies to designated City employees and contractors in the event of a scheduled exercise or an actual emergency.

A major challenge with any business continuity management program is timely and effective emergency notifications – responding to scenarios ranging from full blown disasters to daily employee communications.

Calling individual staff members is slow and inefficient. On average it takes approximately 10 minutes to call one person and let them know, for example, the office is closed due to a fire. As a result, staff further down on the call list may not be notified in time for them to get to a different location in a timely manner. This increases risk to staff safety, unnecessary confusion for staff, increases time spent for the manager returning calls, listening to voicemail, and dealing with disgruntled staff members.

The proposed ENS should allow the City to automate the process of giving employees important information in a time of crisis. The system should allow messages to be individualized to allow managers to send different employees or divisions different messages such as asking them to attend a strategy meeting, leave their premises or simply report their locations.

The ENS should provide the ability to quickly send a notification to a group of people simultaneously and allow for immediate responses. The ENS should also provide an audit trail of delivery receipt and response.

Current State:

Currently, the City does not have an automated or manual process in place to contact all City employees and contractors in the event of an emergency.

The City is looking for an ENS that may be used for situations such as but not limited to:

[End of Page]

Incident/Event response: o Business continuity management (BCM) o Disaster Recovery (DR) o Crisis Management (CM) o Employee safety (ES) o Emergency Response (ERP)	**Communications/Response/Tracking/Safety:** **BCM/DR/CM/ES/ERP** o Speed notification and response times as critical events unfold o Coordinate efforts and link to business continuity plans o Track and bring people together before, during or after a disaster o Facilitate BCM communication exercises o Reduction of business risk and vulnerability o Employee Safety
Information Solutions o Disaster recovery o 1st Line Support o 2nd Line Support	***IS* solutions** o Alert *IS* staff of situation o Automated *IS* notifications through ENS (using devices other than email) **Information Technology** o Automate notifications relating to *IS* service interruptions o Notify users of *IS*-related service disruptions o Coordinate *IS* and Call Centre staff
Call Centres: o IS Service Desk o Customer Contact Centre	**IS Service Desk** o Proactive customer relationship management o Faster, personalised service o Audit trail with customer interaction **The City of Surrey's Customer Contact Center** o Improved Customer Service through timely communications o Send out important information via ENS to ***THE CITY OF SURREY'S*** stakeholders **Staffing** o Use notifications to inform employees of changes to the work schedule
Human Resources:	**Staff Health** o Inform staff of outbreaks or health warnings and include information on precautions and steps to take if infected (e.g. message to staff via ENS in time of pandemic) o Inform staff of travel alerts (before and during travelling)

Business Process:	**Business Operations:** o Generating and managing notifications for any communication dependent business operation o Improve stakeholder relations through timely information – ENS can satisfy any legal notification requirements to stakeholders when disruption is experienced **Scheduling:** o Communicate changes in work schedules o Send severe weather warnings or accident alerts to all locations
Leadership Communications	**Corporate messaging** o Critical messages only

SCHEDULE A-1 – FUNCTIONAL AND TECHNICAL REQUIREMENTS

FUNCTIONAL REQUIREMENTS					
Req. #	**Requirement**	**Elaboration**	**Category**	**Theme**	**Level of Need**
1000	Available as a SaaS solution.	System is available as an Online Software as a Service solution	General	Delivery Solution	Mandatory
1001	Describe any additional delivery models.		General	Delivery Solution	Preferred
1002	The City of Surrey will retain all rights and ownership of data entered on system.		General	Data	Mandatory
1003	Utilizes workstations/laptops, requires no hardware/software installation.	System can run on workstations/laptops/mobile devices with no additional software or hardware installation.	General		Preferred
1004	Upgrades and enhancements provided seamlessly (with no interruption of service) at no additional cost.		General		Preferred
1005	No technical limit on the number contacts.	Ability to enter as many contacts into system as needed.	General	Technical Limit	Preferred
1006	No technical limit on the number distribution lists.	Ability to enter as many distribution lists into system as needed.	General	Technical Limit	Preferred
1007	No technical limit on the number of messages that can be concurrently sent.		General	Technical Limit	Preferred
1008	No technical limit on the number of contacts that may receive any message.		General	Technical Limit	Preferred

1009	No technical limit on the number of contacts in any one distribution list.		General	Technical Limit	Preferred
1010	No technical limit on the number of distributions lists to which one contact may belong.		General	Technical Limit	Preferred
1011	No technical limit on the number of messages that any one contact can concurrently be sent.		General	Technical Limit	Preferred
1012	No technical limit on the number of concurrent users who may access the system.		General	Technical Limit	Preferred
1013	Able to be used with no restrictions for emergency messages.	Ability to send any type of emergency messages	General	Message Restriction	Preferred
1014	Able to be used with no restrictions for Business Continuity/Disaster Recovery (BC/DR) messages.		General	Message Restriction	Preferred
1015	Able to be used with no restrictions for informational messages.		General	Message Restriction	Preferred
1016	Able to be used with no restrictions for IT alerting.		General	Message Restriction	Preferred
1017	Able to be used with no restrictions for operational messaging.		General	Message Restriction	Preferred
1018	Able to be used with no restrictions for other messaging.	Describe other types of messaging available	General	Message Restriction	Preferred
1019	Able to include employees, contractors, customers and other types as contacts without any limitations.	Ability to identify and include different types of contacts, internal and external.	General		Preferred

1020	Able to send "broadcast messages" where every contact included receives the message.		Polling & Response	Broadcast Message	Preferred
1021	Able to send "broadcast messages" where every contact included receives the message one-way, with no response/acknowledgement.		Polling & Response	Broadcast Message	Preferred
1022	Able to send "broadcast messages" where every contact included receives the message two-way, where contact responds by selecting from one or more City of Surrey defined choices.		Polling & Response	Broadcast Message	Preferred
1023	Able to ask follow-up questions based on contact's initial response.		Polling & Response		Preferred
1024	Able to send “polling messages” where each contact is asked to respond to a question or series of questions.		Polling & Response	Polling Message	Preferred
1025	Able to specify limit on number of questions sent on "polling messages".		Polling & Response	Polling Message	Preferred
1026	Describe types of responses available on "polling messages".		Polling & Response	Polling Message	Preferred
1027	Able to send "quota messages" that end after enough contacts respond with a "yes" response.		Polling & Response	Quota Message	Preferred
1028	Able to specify how many "yes" responses are required on "quota messages".		Polling & Response	Quota Message	Preferred
1029	Able to use City of Surrey defined response text for both "yes" and "no responses on "quota messages".		Polling & Response	Quota Message	Preferred

1030	Able to include multiple responses for "yes", such as "Yes, immediately" and "Yes, within 30 minutes" on "quota messages".		Polling & Response	Quota Message	Preferred
1031	Able to send "quota messages" immediately to all contacts, or to contact small groups at a time.		Polling & Response	Quota Message	Preferred
1032	Able to define who should be contacted first, second, etc. (tiered contacts) in an escalation process, and the maximum time before moving to the next tier on "quota messages".		Polling & Response	Quota Message	Preferred
1033	Able to "post" messages for contacts to hear by calling into a toll-free IVR phone number		Polling & Response		Preferred
1034	Able to use all features available for a dial-out message - describe any differences.		Polling & Response		Preferred
1035	Able to search and select individual contacts and/or distribution lists and on-call schedules to receive each message		Polling & Response		Preferred
1036	Able to send to all contacts in any allowed distribution lists, even if not allowed to directly see/select the contacts who are members		Polling & Response		Preferred
1037	Able to send a message to contacts who have subscribed to that type of message, in addition to/in place of directly selecting those contacts		Polling & Response		Preferred

1038	Recognizes that the same contact has been included via multiple distribution lists and does not contact that individual multiple times.		Polling & Response		Preferred
1039	Provides an option to only contact each unique phone number, SMS text device, email, etc. once -- even if multiple contacts have that same device in their profiles, such as a switchboard or group work-area number/email	Provides an option to only contact each unique phone number, SMS text device, email, etc. once -- even if multiple contacts have that same communication method (i.e. email, text, etc.) in their profiles, such as a switchboard or group work-area number/email	Polling & Response		Preferred
1040	Able to join contacts to a conference call.		Polling & Response	Conference Call	Preferred
1041	Able to join contacts to a conference call without the contact knowing/entering any conference detail.		Polling & Response	Conference Call	Preferred
1042	Able to join contacts to a conference call using the City of Surreys' standard conference service	Describe conference services supported. i.e. Microsoft Teams	Polling & Response	Conference Call	Preferred
1043	Able to join contacts to a conference call with ability to specify maximum number of contacts able to be joined.		Polling & Response	Conference Call	Preferred
1044	Able to select a second message to be automatically sent when/if a contact chooses a designated response.		Polling & Response		Preferred
1045	Device support for various types of Phones (land lines, cell phones, smart phones, satellite phones, VoIP phones)		Contact Device (Communication Method) Support	Device Support	Preferred
1046	Device support for Email	Able to support Email communication.	Contact Device (Communication Method) Support	Device Support	Preferred

1047	Device support for SMS 1-way support (via SMTP)	Able to provide SMS 1-way support (via SMTP) communication	Contact Device (Communication Method) Support	Device Support	Preferred
1048	Device support for SMS 1-way support (via SMPP)	Able to provide SMS 1-way support (via SMPP) communication	Contact Device (Communication Method) Support	Device Support	Preferred
1049	Device support for SMS 2-way support (via SMPP)	Able to provide SMS 2-way support (via SMPP) to devices	Contact Device (Communication Method) Support	Device Support	Preferred
1050	Device support for Mobile app	Able to support Mobile app communication	Contact Device (Communication Method) Support	Device Support	Preferred
1051	Device support for Blackberry PIN-to-PIN	Able to support Blackberry PIN-to-PIN communication	Contact Device (Communication Method) Support	Device Support	Preferred
1052	Device support for Pager - numeric	Able to support Pager - numeric communication	Contact Device (Communication Method) Support	Device Support	Preferred
1053	Device support for Pager – 1-way	Able to support Pager – 1-way communication	Contact Device (Communication Method) Support	Device Support	Preferred
1054	Device support for Pager – 2-way	Able to support for Pager – 2-way communication	Contact Device (Communication Method) Support	Device Support	Preferred
1055	Device support for TTY/TTD	Able to support TTY/TTD communication	Contact Device (Communication Method) Support	Device Support	Preferred
1056	Device support for FAX	Able to support FAX communication	Contact Device (Communication Method) Support	Device Support	Preferred
1057	Device support for Desktop alerts - describe if native or 3rd party involved	Able to support communication with Desktop alerts. Describe if native or 3rd party involved	Contact Device (Communication Method) Support	Device Support	Preferred

1058	Device support for Social media	Able to support communication by Social media	Contact Device (Communication Method) Support	Device Support	Preferred
1059	Device support for Digital signage	Able to support Digital signage communication	Contact Device (Communication Method) Support	Device Support	Preferred
1060	Device support for RSS reader	Able to support communication with RSS reader	Contact Device (Communication Method) Support	Device Support	Preferred
1061	Supports international messaging on all devices. Describe any limitations.	Supports international messaging on all communication methods. i.e.; email, mobile # Describe any limitations.	Contact Device (Communication Method) Support		Desired
1062	Supports multiple versions of a message for different devices, sent automatically in one action.	Supports multiple versions of a message for different communication methods, sent automatically in one action. i.e.; email, mobile #	Contact Device (Communication Method) Support		Preferred
1063	Provides delivery of voice messages using high quality, easily understandable Text-to-Speech (TTS) engine.		Contact Device (Communication Method) Support		Preferred
1064	Simultaneous delivery of messages in multiple languages, according to recipient's language selection. Please list languages supported.		Contact Device (Communication Method) Support		Preferred
1065	Supports voice-recorded messages on all phone devices. Describe recording process.		Contact Device (Communication Method) Support		Preferred
1066	Provides IVR call-back to hear and respond to missed messages.		Contact Device (Communication Method) Support	IVR Call-back	Preferred

1067	Able to control how long a message will remain open for call-back		Contact Device (Communication Method) Support	IVR Call-back	Preferred
1068	Specify maximum time message may remain open for contacts to use the call-back to hear messages and/or respond		Contact Device (Communication Method) Support	IVR Call-back	Preferred
1069	Able to determine if voicemail/answering machine reached instead of a live person.		Contact Device (Communication Method) Support	Voicemail	Preferred
1070	Able to control if a message is left on voicemail/answering machine		Contact Device (Communication Method) Support	Voicemail	Preferred
1071	Able to leave a message tailored for voicemail/answering machines		Contact Device (Communication Method) Support	Voicemail	Preferred
1072	Able to have IVR call-back number left as part of message	Ability to provide Interactive Voice Response (IVR) call-back number for contact to respond back to as part of message.	Contact Device (Communication Method) Support	Voicemail	Preferred
1073	Able for sender to determine how devices are contacted for each message.	Ability for sender to determine which communication methods are used to send each message. For example; email, text	Contact Device (Communication Method) Support	Communication Method	Preferred
1074	Able to send to devices simultaneously - all or selected devices.	Able to send to all or selected communication methods (i.e.; email, text, etc.) simultaneously	Contact Device (Communication Method) Support	Communication Method	Preferred

1075	Able to send to devices in a desired order - all or selected devices.	Ability to send messages in desired order of communication method to all or to communication method selected by sender.	Contact Device (Communication Method) Support	Communication Method	Preferred
1076	Able for each contact to determine how their own devices are contacted.	Ability for contact to specify their preferred method of contact by priority. i.e. 1) mobile #, 2) text	Contact Device (Communication Method) Support	Communication Method	Preferred
1077	Support additional authentication of contacts before delivering phone messages.	Describe additional authentication.	Contact Device (Communication Method) Support		Preferred
1078	Able to receive confirmation from contacts		Contact Device (Communication Method) Support		Preferred
1079	Able to receive confirmation from contacts on all devices above - describe any limitation	Able to receive confirmation from contacts on all communication methods above. Describe any limitation.	Contact Device (Communication Method) Support	Confirmation	Preferred
1080	Able to receive confirmation from contacts using City of Surrey defined responses - describe maximum allowed		Contact Device (Communication Method) Support	Confirmation	Preferred
1081	Able to assign a limit to the number of attempts made to reach individuals for each message and specify the wait time between attempts.		Contact Device (Communication Method) Support		Preferred
1082	Able to stop contacting a person once a response received from any device or via the IVR	Able to stop contacting a person once a response received from any communication method or via the IVR	Contact Device (Communication Method) Support	Stop Contact	Preferred

1083	Able to stop contacting a person after the person has listened to the message		Contact Device (Communication Method) Support	Stop Contact	Preferred
1084	Able to stop contacting a person after a voicemail has been left		Contact Device (Communication Method) Support	Stop Contact	Preferred
1085	Able to contact a person's listed alternates if the person cannot be reached.		Contact Device (Communication Method) Support	Contact Alternate	Preferred
1086	Able to offer the option to contact a person's listed alternates when receiving a message; for a person to indicate their alternates should be contacted in their place		Contact Device (Communication Method) Support	Contact Alternate	Preferred
1087	Able to attach and send documents to a text-based device.	Able to attach and send documents to a text-based communication method.	Contact Device (Communication Method) Support		Preferred
1088	Able to post IVR "bulletin board" messages for only targeted contacts, with authentication - describe	Describe how IVR "bulletin board" messages are targeted and authenticated.	Contact Device (Communication Method) Support	Bulletin Board	Preferred
1089	Able to post IVR "bulletin board" messages for anyone dialing the number		Contact Device (Communication Method) Support	Bulletin Board	Preferred
1090	Provide inbound IVR numbers to call-back for missed messages and/or hear posted "bulletin board" messages, Toll-free in the US/Canada		Contact Device (Communication Method) Support	Inbound IVR	Preferred
1091	Provide inbound IVR numbers to call-back for missed messages and/or hear posted "bulletin board" messages, Toll-based in the US/Canada		Contact Device (Communication Method) Support	Inbound IVR	Preferred

1092	Provide inbound IVR numbers to call-back for missed messages and/or hear posted "bulletin board" messages, toll-free internationally - describe coverage		Contact Device (Communication Method) Support	Inbound IVR	Preferred
1093	Provide inbound IVR numbers to call-back for missed messages and/or hear posted "bulletin board" messages, Toll-based internationally		Contact Device (Communication Method) Support	Inbound IVR	Preferred
1094	Provide inbound IVR numbers to call-back for missed messages and/or hear posted "bulletin board" messages; automatic authentication of inbound callers based on their telephone’s caller ID		Contact Device (Communication Method) Support	Inbound IVR	Preferred
1095	Provide inbound IVR numbers to call-back for missed messages and/or hear posted "bulletin board" messages; prompted authentication when no caller ID or the caller ID not recognized		Contact Device (Communication Method) Support	Inbound IVR	Preferred
1096	Provide inbound IVR numbers to call-back for missed messages and/or hear posted "bulletin board" messages; optionally require a PIN to be entered before message delivery		Contact Device (Communication Method) Support	Inbound IVR	Preferred
1097	Ability to enter/support contact attribute: Unique ID (employee ID or other value)		Contact Data	Contact Attributes	Preferred
1098	Ability to enter/support contact attribute: Last Name		Contact Data	Contact Attributes	Preferred
1099	Ability to enter/support contact attribute: First Name		Contact Data	Contact Attributes	Preferred

1100	Ability to enter/support contact attribute: Contact Devices - describe maximum number per contact, any limitation on how many of each type device	Include communication methods in contact attributes. Describe maximum number per contact. Are there limitations on how many of each communication method? i.e.; email, mobile #, land #, all contact #'s	Contact Data	Contact Attributes	Preferred
1101	Ability to enter/support contact attribute: Title		Contact Data	Contact Attributes	Preferred
1102	Ability to enter/support contact attribute: Company/Organization		Contact Data	Contact Attributes	Preferred
1103	Ability to enter/support contact attribute: Department		Contact Data	Contact Attributes	Preferred
1104	Ability to enter/support contact attribute: Division		Contact Data	Contact Attributes	Preferred
1105	Ability to enter/support contact attribute: Language Preference		Contact Data	Contact Attributes	Preferred
1106	Ability to enter/support contact attribute: Time Zone		Contact Data	Contact Attributes	Preferred
1107	Ability to enter/support contact attribute: Username/Password (for ENS Software login)		Contact Data	Contact Attributes	Preferred
1108	Ability to enter/support contact attribute: PIN Number (for phone authentication)		Contact Data	Contact Attributes	Preferred

1109	Ability to enter/support contact attribute: Address fields, including description, address/city/country/etc. - describe types of addresses supported		Contact Data	Contact Attributes	Preferred
1110	Ability to enter/support contact attribute: Alternates, selected from other contacts and ordered as desired.		Contact Data	Contact Attributes	Preferred
1111	Able to add additional fields to the contact record, to meet all City of Surrey specific purposes. Specify how many allowed.		Contact Data	Contact Attributes	Preferred
1112	Ability to enter/support skills matrix and certifications		Contact Data	Contact Attributes	Desired
1113	Privacy setting on devices and addresses hides the device address (phone number, email address, etc.) and/or physical address from users who are not granted 'private access'.	Leave privacy settings as specified by user.	Contact Data	Contact Attributes	Preferred
1114	Address geo-coding supported, automatic at time of add/update of any address, including during import		Contact Data	Geo-coding	Preferred
1115	Address geo-coding supported for full and partial addresses, such as only city/state/country		Contact Data	Geo-coding	Preferred
1116	Address geo-coding supported during interactive input, choices offered if address cannot be geocoded as entered	Provide alternate choices if geocoding cannot be resolved.	Contact Data	Geo-coding	Preferred

1117	Hierarchical data structure definable by City of Surrey		Contact Data	Hierarchical Data	Preferred
1118	Hierarchical data structure definable by City of Surrey based on location, organizational structure, functional areas, etc.		Contact Data	Hierarchical Data	Preferred
1119	Hierarchical data structure definable by City of Surrey based on a combination of the above		Contact Data	Hierarchical Data	Preferred
1120	Hierarchical data structure definable by City of Surrey with unlimited levels		Contact Data	Hierarchical Data	Preferred
1121	Hierarchical data structure definable by City of Surrey with unlimited number of 'nodes' (entries) at each level		Contact Data	Hierarchical Data	Preferred
1122	Hierarchical data structure definable by City of Surrey where different areas of the structure can have different sets of levels if needed (such as a State level under the USA node, but none for State under other country nodes)		Contact Data	Hierarchical Data	Preferred
1123	Hierarchical data structure definable by City of Surrey where contacts, distribution lists, messages and all other city data assigned to a node in the structure		Contact Data	Hierarchical Data	Preferred
1124	Able to update contact data with manual entry by an authorized user		Data Management	Update Contact	Preferred
1125	Able to update contact data with manual import by an authorized user, using Excel/CSV file input		Data Management	Update Contact	Preferred

1126	Able to update contact data with automated import process		Data Management	Update Contact	Preferred
1127	Able to update contact data with self-management portal for contacts to edit own record		Data Management	Update Contact	Preferred
1128	Able to update contact data with integrations from City of Surrey applications/systems using an API		Data Management	Update Contact	Preferred
1129	Able to update contact data with combination of methods (import core data, contacts add own data, integrated application updates relevant data)		Data Management	Update Contact	Preferred
1130	Able to update contact data by other means	Describe other ways to update contact data that your system offers.	Data Management	Update Contact	Preferred
1131	Automated import process provides ability to use data from any source, including feeds from any HR system, external database or other system containing contact data	Specify what systems are supported for importing of data. i.e.; Peoplesoft, Active Directory, SQL Database	Data Management	Automated Import	Preferred
1132	Automated import process provides ability to use data from Peoplesoft.	Peoplesoft is an on-premise application the city uses for Human Resources.	Data Management	Automated Import	Preferred
1133	Ability to connect to ESRI/GIS system.	Ability to connect to city's ESRI/GIS system via an API. ESRI/GIS is an on-premise application the city uses for mapping.	Data Management	Interface	Desired

1134	Automated import process provides ability to directly connect to and import data from LDAP (Lightweight Directory Access Protocol) directories such as Active Directory		Data Management	Automated Import	Preferred
1135	Automated import process provides addition of new contacts		Data Management	Automated Import	Preferred
1136	Automated import process provides automatic removal of contacts no longer in the import source, such as persons no longer with company		Data Management	Automated Import	Preferred
1137	Automated import process provides ability to manage contact membership on distribution lists		Data Management	Automated Import	Preferred
1138	Automated import process provides scheduling as needed (daily, weekly, etc.) at a desired time of day		Data Management	Automated Import	Preferred
1139	Automated import process provides no interruption in usage of the system, including sending messages, while import is underway		Data Management	Automated Import	Preferred
1140	Automated import process provides full log files of all import results, including data issues		Data Management	Automated Import	Preferred

1141	Self-management web portal page provides secure login to manage own contact profile		Data Management	Self-management	Preferred
1142	Self-management web portal page provides configuration to City of Surrey requirements on what data is viewable, editable by contacts		Data Management	Self-management	Preferred
1143	Self-management web portal page provides ability for person to edit data fields and add/update/delete devices in their own record	Self-management web portal page provides ability for person to edit data fields and add/update/delete communication methods in their own record	Data Management	Self-management	Preferred
1144	Self-management web portal page provides ability for person to set the standard order for their own devices to be contacted, including turning devices off and/or defining different orders for different times/days during the week	Self-management web portal page provides ability for person to set the standard order for their own communication methods to be contacted.	Data Management	Self-management	Preferred
1145	Self-management web portal page provides ability to subscribe to the types of messages the person wishes to receive		Data Management	Self-management	Preferred
1146	Self-management web portal page provides optional approval process for all subscriptions entered by users		Data Management	Self-management	Preferred
1147	Self-management web portal page provides coordination with the automated import, allowing data entered in the portal to be preserved each time the import executes		Data Management	Self-management	Preferred

1148	Able to add a temporary travel or work location through a map on the mobile app or in the web interface, including an expiration for that location		Data Management		Preferred
1149	Explicit opt-in process supported for contact's SMS devices	Explicit opt-in process supported for contact's SMS communication methods	Data Management		Preferred
1150	Able to search and select contacts		Data Management	Search	Preferred
1151	Able to search and select contacts based on any information in the contact record		Data Management	Search	Preferred
1152	Able to search and select contacts using an exact match, the first letter of the Last Name or a wildcard match (such as 553* for a Zip Code search for all starting with 553)		Data Management	Search	Preferred
1153	Able to search and select contacts using 'search within last search results', such as show me everyone who lives in New York, followed by show me all those in Building 5, 6th floor, who were qualified from the first search of New York.		Data Management	Search	Preferred
1154	Able to search and select contacts in multiple ways, and include each set of search results in the final set of contacts selected		Data Management	Search	Preferred

1155	Able to export all/selected contact records to an Excel/CSV file, including all fields and devices	Ability to export all/select contact records to an Excel/CSV file, including all fields and all communication methods.	Data Management	Search	Preferred
1156	Able to use predefined distribution lists to quickly select the contacts to receive a message		Distribution List Management	Supported	Preferred
1157	Able to include any contact in a distribution list, as long as the user's security allows it		Distribution List Management	Supported	Preferred
1158	Distribution lists supported include static lists with a selected group of members		Distribution List Management	Supported	Preferred
1159	Distribution lists supported include dynamic lists based on a search/query criteria on any contact attribute		Distribution List Management	Supported	Preferred
1160	Distribution lists supported include GIS lists defined by drawing shapes on a map		Distribution List Management	Supported	Preferred
1161	Distribution lists supported include on-call schedules, defining who should be contacted at any given day/time when a message is sent to the schedule		Distribution List Management	Supported	Preferred
1162	Distributions list updated by interactive update by an authorized user		Distribution List Management	Update	Preferred
1163	Distributions list updated as part of a manual contact import		Distribution List Management	Update	Preferred

1164	Distributions list updated as part of the automated, scheduled contact import		Distribution List Management	Update	Preferred
1165	Distributions list updated by import of a list of member email addresses		Distribution List Management	Update	Preferred
1166	Able to interactively create/manage distribution lists		Distribution List Management		Preferred
1167	Able to search for distribution lists based on a wildcard search of the name, such as *Phoenix* for all lists with a name containing Phoenix		Distribution List Management		Preferred
1168	Able to export to a CSV file the members of one or more distribution lists, with their contact data included		Distribution List Management		Preferred
1169	Able to support Static distribution lists		Distribution List Management	Static List	Preferred
1170	Static lists provide no limit on the number of members		Distribution List Management	Static List	Preferred
1171	Static lists provide inclusion of any mixture of individual contacts and other lists		Distribution List Management	Static List	Preferred
1172	Static lists provide hierarchy of nested lists - describe any limit		Distribution List Management	Static List	Preferred
1173	Able to support Dynamic distribution lists		Distribution List Management	Dynamic List	Preferred
1174	Dynamic lists provide search criteria based on any contact attribute, including custom fields		Distribution List Management	Dynamic List	Preferred
1175	Dynamic lists provide complex searches using AND/OR/NOT		Distribution List Management	Dynamic List	Preferred
1176	Dynamic lists provide inclusion of other lists based on name searches		Distribution List Management	Dynamic List	Preferred

1177	Dynamic lists provide automatic refresh of the membership based on the search criteria, each time the list is used in any way		Distribution List Management	Dynamic List	Preferred
1178	Able to support GIS (Geographic Information System) lists		Distribution List Management	GIS List	Preferred
1179	GIS lists provide display of all contact addresses/locations on a map		Distribution List Management	GIS List	Preferred
1180	GIS lists provide world-wide map support offering a street view, satellite view, terrain view, and a combination of streets and satellite view (hybrid view)		Distribution List Management	GIS List	Preferred
1181	GIS lists provide ability to center/zoom the map on an address, intersection or landmark		Distribution List Management	GIS List	Preferred
1182	GIS lists support drawing, using as many circular, rectangular, and polygon shapes as needed to select region(s) on the map		Distribution List Management	GIS List	Preferred
1183	GIS lists can add an unlimited number of optional, external WMS (Web Mapping Service) display layers (such as live NOAA weather radar, City of Surreys' own map layers such as building locations, pipelines, etc.)		Distribution List Management	GIS List	Preferred
1184	GIS lists can selectively turn-on or turn-off any City of Surrey included WMS layers		Distribution List Management	GIS List	Preferred
1185	Able to support On-call schedules		Distribution List Management	On-call Schedules	Preferred
1186	On-call schedules provide shift definitions, which define the times when a group of people are on-call and who is on call		Distribution List Management	On-call Schedules	Preferred

1187	On-call schedules provide escalations within each shift, identifying who is called first/second/etc. (tiers) and the maximum time to attempt reaching someone at each tier		Distribution List Management	On-call Schedules	Preferred
1188	On-call schedules support recurrence of each shift, including every weekday/weekend, first/last/etc. of month/quarter/etc., and a rotating pattern of days (4 days on and 2 days off, every other week on Mon-Fri, etc.)		Distribution List Management	On-call Schedules	Preferred
1189	On-call schedules provide visual display of current coverage by shifts, to assist in identifying 'holes' in coverage		Distribution List Management	On-call Schedules	
1190	On-call schedules provide ability to easily define exceptions, when someone is on Paid Time Off (PTO) or out for a few hours during an assigned shift		Distribution List Management	On-call Schedules	Preferred
1191	Create and store an unlimited number of template messages for future usage.		Message Creation/Sending	Template Message	Preferred
1192	Copy an existing template message to easily create a new, similar message.		Message Creation/Sending	Template Message	Preferred
1193	Ability to use and modify vendor provided templates.		Message Creation/Sending	Template Message	Preferred
1194	Messages can be created by an interactive user on any workstation/laptop or tablet with a standard browser		Message Creation/Sending	Message Creation	Preferred
1195	Messages can be created by mobile app on a smartphone or tablet		Message Creation/Sending	Message Creation	Preferred
1196	Messages can be created by an integrated external system or application		Message Creation/Sending	Message Creation	Preferred

1197	Messages can be sent by an interactive user on any workstation/laptop or tablet with a standard browser	An interactive user is anyone with access to the system.	Message Creation/Sending	Messages Sent	Preferred
1198	Messages can be sent at a scheduled time, recurring if desired		Message Creation/Sending	Messages Sent	Preferred
1199	Messages can be sent by an email to the system - describe the process		Message Creation/Sending	Messages Sent	Preferred
1200	Messages can be sent by an integrated external system or application		Message Creation/Sending	Messages Sent	Preferred
1201	Messages can be sent by a user calling a touch-tone phone number, and answering prompts with a press of a key		Message Creation/Sending	Messages Sent	Preferred
1202	Messages can be sent by mobile app on a smartphone or tablet		Message Creation/Sending	Messages Sent	Preferred
1203	Messages can be sent by contacting a live vendor support representative 24x7x365		Message Creation/Sending	Messages Sent	Preferred
1204	Interactive users send messages on-the-fly by selecting those to receive the message (recipients) and entering the message, and nothing more		Message Creation/Sending	Send Message	Preferred
1205	Interactive users send messages using a predefined message template, with all recipients and delivery options already specified		Message Creation/Sending	Send Message	Preferred
1206	Interactive users send messages by temporarily editing a predefined message template, and sending without saving		Message Creation/Sending	Send Message	Preferred
1207	Interactive users send messages by defining a new message template		Message Creation/Sending	Send Message	Preferred

1208	Interactive users send messages by using form with dropdown choices and/or text entry fields, and those values can construct/modify the message and select recipients		Message Creation/Sending	Send Message	Preferred
1209	Provides an embedded weather interface, allowing automatic messages to be sent to any number of contacts when designates types of weather occur in geofenced areas of interest		Message Creation/Sending		Preferred
1210	User able to send a message test to only themselves without editing the message setup in any way		Message Creation/Sending		Preferred
1211	Able to cancel in-process messages at any time.		Message Creation/Sending	Cancel Message	Preferred
1212	Able to cancel in-process messages at any time from the web interface		Message Creation/Sending	Cancel Message	Preferred
1213	Able to cancel in-process messages at any time using the mobile app		Message Creation/Sending	Cancel Message	Preferred
1214	Able to cancel in-process messages at any time by an integrated external system or application		Message Creation/Sending	Cancel Message	Preferred
1215	Able to prioritize emergency messages standard messages.		Message Creation/Sending		Preferred
1216	Able to send a second message to only those who did not respond to the original message.		Message Creation/Sending		Preferred
1217	Supports a sender alias, in voice announcements and as the email FROM 'human name' portion		Message Creation/Sending		Preferred
1218	Able to configure phone delivery options for each message as needed		Message Creation/Sending	Configure Phone Delivery	Preferred

1219	Able to configure phone delivery options for each message to include a personal greeting		Message Creation/Sending	Configure Phone Delivery	Preferred
1220	Able to configure phone delivery options for each message to require contact to confirm their response choice		Message Creation/Sending	Configure Phone Delivery	Preferred
1221	Able to configure phone delivery options for each message to allow user to replay the message		Message Creation/Sending	Configure Phone Delivery	Preferred
1222	Able to configure phone delivery options for each message to allow language selection, of the languages in which the message was created		Message Creation/Sending	Configure Phone Delivery	Preferred
1223	Able to configure phone delivery options for each message to validate that the correct person answered the phone		Message Creation/Sending	Configure Phone Delivery	Preferred
1224	Able to configure phone delivery options for each message to provide an opportunity for the person answering to indicate that the number doesn't belong to the intended contact		Message Creation/Sending	Configure Phone Delivery	Preferred
1225	Able to configure textual (non-phone) delivery options for each message as needed		Message Creation/Sending	Configure Textual Delivery	Preferred
1226	Able to configure textual (non-phone) delivery options for each message to limit to only one message to each device, even if phones will continue to be contacted multiple times		Message Creation/Sending	Configure Textual Delivery	Preferred
1227	Able to configure textual (non-phone) delivery options for each message to set the time to wait for a response, before assuming no immediate response and moving to the next device(s)		Message Creation/Sending	Configure Textual Delivery	Preferred

1228	Able to optionally use alternates for each contact not reached		Message Creation/Sending		Preferred
1229	Able to allow a contact who was reached to indicate their alternates should be contacted in their place		Message Creation/Sending		Preferred
1230	Able to group a number of related but different messages, that can be sent together automatically.		Message Creation/Sending		Preferred
1231	Provides real-time dashboard display of a message's progress.		Monitoring/Reporting	Real-time Dashboard	Preferred
1232	Provides real-time dashboard display of a message's progress with automatic refresh every few seconds	Describe refresh rate	Monitoring/Reporting	Real-time Dashboard	Preferred
1233	Provides real-time dashboard display of a message's progress which includes title, message, sender and date sent	Describe attributes available on dashboard.	Monitoring/Reporting	Real-time Dashboard	Preferred
1234	Provides real-time dashboard display of a message's progress which includes summary of how many individuals contacted, including counts of those who responded, have not responded or were not able to be contacted		Monitoring/Reporting	Real-time Dashboard	Preferred
1235	Provides real-time dashboard display of a message's progress displaying statistics including the number of each type of device contacted, etc.	Provides real-time dashboard display of a message's progress displaying statistics including the number of each communication method contacted.	Monitoring/Reporting	Real-time Dashboard	Preferred

1236	Provides real-time dashboard display of a message's progress to report on each contact attempt made, including who, when, on what device, and the results of that attempt	Provides real-time dashboard display of a message's progress to report on each contact attempt made, including who, when, on what communication method, and the results of that attempt	Monitoring/Reporting	Real-time Dashboard	Preferred
1237	Provides real-time dashboard display of a message's progress to detect and report busy signals, hang-ups, no-answers, voicemails, etc. for phone calls		Monitoring/Reporting	Real-time Dashboard	Preferred
1238	Provides real-time dashboard display of a message's progress to detect and report when SMS text messages are sent, delivered or are in-progress with the aggregator or carrier		Monitoring/Reporting	Real-time Dashboard	Preferred
1239	Provides real-time dashboard display of a message's progress to detect and report automated email kick-back replies		Monitoring/Reporting	Real-time Dashboard	Preferred
1240	Provides real-time dashboard display of a message's progress showing responses/confirmations logged with a timestamp for each contact		Monitoring/Reporting	Real-time Dashboard	Preferred
1241	Provides real-time dashboard display of a message's progress with ability to map display of saved locations/addresses for all those included to receive the message		Monitoring/Reporting	Real-time Dashboard	Preferred

1242	Provides real-time dashboard display of a message's progress with ability to target contacts for another message, based on how they responded (or didn't)		Monitoring/Reporting	Real-time Dashboard	Preferred
1243	Provides real-time dashboard display of a message's progress with ability to export results to CSV, PDF or Excel file format		Monitoring/Reporting	Real-time Dashboard	Preferred
1244	Supports automatic emailed report for each sent message.		Monitoring/Reporting	Automatic Emailed Report	Preferred
1245	Sender automatically receives report on completion of sent message		Monitoring/Reporting	Automatic Emailed Report	Preferred
1246	Device to receive automatic emailed report of sent message can be selected for each user	Each user can select communication method to receive automatic emailed report of sent message	Monitoring/Reporting	Automatic Emailed Report	Preferred
1247	Able to have the automatic emailed report of sent message sent to any set of contacts and/or distribution lists		Monitoring/Reporting	Automatic Emailed Report	Preferred
1248	Automatic emailed report of sent message can be in plain text, CSV and PDF format		Monitoring/Reporting	Automatic Emailed Report	Preferred
1249	Automatic emailed report of sent message can be optionally sent at regular intervals while the message is still active		Monitoring/Reporting	Automatic Emailed Report	Preferred
1250	Online history available for each completed message.		Reporting	Online History	Preferred
1251	Online history available for each completed message to be retained for at least 18 months		Reporting	Online History	Preferred

1252	Online history available for each completed message; Differences in functionality from real-time dashboard - describe.	Difference from historical to real-time dashboards	Reporting	Online History	Preferred
1253	Able to search for groups of related message reports based on timeframe sent.		Reporting	Search Related Messages	Preferred
1254	Able to search for groups of related message reports based on message/title text		Reporting	Search Related Messages	Preferred
1255	Able to search for groups of related message reports based on sender		Reporting	Search Related Messages	Preferred
1256	Able to search for groups of related message reports based on specific user(s) who received the message		Reporting	Search Related Messages	Preferred
1257	Able to export a consolidated report on a group of messages.		Reporting		Preferred
1258	Able to search audit trail history.		Reporting	Search Audit History	Preferred
1259	Able to search audit trail history by user who took the action		Reporting	Search Audit History	Preferred
1260	Able to search audit trail history by type of action		Reporting	Search Audit History	Preferred
1261	Able to search audit trail history by the timeframe of the action		Reporting	Search Audit History	Preferred
1262	Able to search audit trail history for updates to specific data records		Reporting	Search Audit History	Preferred
1263	Able to search audit trail history and export results to CSV or Excel file format		Reporting	Search Audit History	Preferred

1264	Provides a detailed usage report for a selected time period, including all device contact attempt.		Reporting		Preferred
1265	No limit on which contacts can be system users		User Security		Preferred
1266	System login available using unique assigned login ID, and password		User Security	System Login	Preferred
1267	System login available using Single Sign On (SSO)		User Security	System Login	Preferred
1268	System login available using LDAP Authentication (with no credentials stored in ENS Software)		User Security	System Login	Preferred
1269	May assign any user a security role to use the system.		User Security	Security Role	Preferred
1270	Standard security roles provided - describe	Describe standard security roles provided.	User Security	Security Role	Preferred
1271	Able to configure custom security roles developed by City of Surrey - describe	Ability to customize security roles. Describe how this is done.	User Security	Security Role	Preferred
1272	Custom templates developed by City of Surrey, that can be combined to build security roles from standard rights sets - describe	Ability to develop custom templates that can be combined to build security roles from standard rights sets. Describe how this can be done.	User Security	Security Role	Preferred
1273	No limit on number of security custom roles or templates		User Security	Security Role	Preferred
1274	No limit on number of users with any specific role, including System Administrator		User Security	Security Role	Preferred
1275	Assigned role controls overall actions allowed		User Security	Assigned Role Control	Preferred

1276	Assigned role controls overall actions allowed, including sending a message using the web interface or mobile app		User Security	Assigned Role Control	Preferred
1277	Assigned role controls overall actions allowed, including sending a message using a touch-tone phone		User Security	Assigned Role Control	Preferred
1278	Assigned role controls overall actions allowed, including sending a message using an email trigger		User Security	Assigned Role Control	Preferred
1279	Assigned role controls overall actions allowed, including manage/grant access of other users		User Security	Assigned Role Control	Preferred
1280	Assigned role controls overall actions allowed, including performing administrative functions		User Security	Assigned Role Control	Preferred
1281	Assigned role controls overall actions allowed, including other - describe	Describe other role controls available.	User Security	Assigned Role Control	Preferred
1282	Assigned role determines contact access		User Security	Contact Access	Preferred
1283	View contacts for assigned areas of responsibility in the data hierarchy	Based on assigned role, ability to view contacts for assigned areas of responsibility in the data hierarchy	User Security	Contact Access	Preferred
1284	Right to edit and/or delete and/or create contacts in each area	Based on assigned role, the right to edit and/or delete and/or create contacts in each area	User Security	Contact Access	Preferred
1285	Right to import and/or export	Based on assigned role, the right to import and/or export data in the system	User Security	Contact Access	Preferred
1286	Assigned role determines access to template messages, distribution lists and report history		User Security	Assigned Role Access	Preferred

1287	Based on assigned role ability to use and/or build/modify distribution lists for assigned areas of responsibility in the data hierarchy		User Security	Assigned Role Access	Preferred
1288	Based on assigned role ability to initiate and/or build/modify template messages for assigned areas of responsibility in the data hierarchy		User Security	Assigned Role Access	Preferred
1289	Based on assigned role, user can view reports for messages they send		User Security	Assigned Role Access	Preferred
1290	Based on assigned role, user can view all reports for assigned areas of responsibility in the data hierarchy		User Security	Assigned Role Access	Preferred
1291	Password rules enforced	Enforcement of defined password rules	User Security	Password Rules	Preferred
1292	Password rules to enforce a strong password	Strong passwords to be based on City password rules	User Security	Password Rules	Preferred
1293	Password rules to include time expiration. Password must be changed periodically.		User Security	Password Rules	Preferred
1294	Password rules to include lockout rule. Lockout after a number of invalid login attempts	After x failed attempts at logging in, account will be locked.	User Security	Password Rules	Preferred
1295	Able to configure password rules - describe options available		User Security	Password Rules	Preferred
1296	Users can securely reset own password		User Security	Password Rules	Preferred
1297	Resetting own password can be allowed to some, all or no users		User Security	Password Rules	Preferred
1298	Able to set defaults for all delivery options for new messages		Administrative/Configuration Functions		Preferred

1299	Prevent any/all options from being changed in a message		Administrative/Configuration Functions		Preferred
1300	Able to customize device classifications (Work Phone, Mobile Phone, Home Phone, etc.) of devices to be stored - describe maximum number.		Administrative/Configuration Functions		Preferred
1301	May determine types of address (Work, Home, Remote Office, Travel, etc.) to be collected - describe maximum number.	Able to configure different address types (Work, Home, Remote Office, Travel, etc.). Describe maximum number allowed.	Administrative/Configuration Functions		Preferred
1302	Able to correct TTS (text-to-speech) pronunciation in all languages		Administrative/Configuration Functions		Preferred
1303	Able to customize all email, voice and SMS prompts/standard text, globally and/or for specific areas of the data structure.		Administrative/Configuration Functions	Customize Message	Preferred
1304	Able to define layout of email messages, using HTML to format text, add logos/images, include headers/footers, etc.		Administrative/Configuration Functions	Customize Message	Preferred
1305	Configure email to automatically modify prompts/standard text for each message based on the values filled in by the sender for prompted fields during the send		Administrative/Configuration Functions	Customize Message	Preferred
1306	May set the Caller ID(s) used, globally and/or for notifications for specific areas of the data structure.		Administrative/Configuration Functions		Preferred
1307	May set the maximum number of calls to be made to a specific number (or number prefix such as 888-456-98 that will include every call made to a number starting with that prefix).		Administrative/Configuration Functions		Preferred

1308	Able to define an unlimited number of categories used for subscriptions.		Administrative/Configuration Functions		Preferred
1309	Vendor has full BC/DR (Business Continuity/Disaster Recovery) plan in place for all services proposed.		Infrastructure		Preferred
1310	Provide implementation assistance.	Is implementation assistance available? Describe type of implementation assistance.	Implementation	Implementation Assistance	Preferred
1311	Implementation assistance provided for major steps/tasks covered	Describe implementation assistance provided for major steps/tasks.	Implementation	Implementation Assistance	Preferred
1312	Implementation assistance provided for City of Surrey vs. vendor responsibilities	Describe City of Surrey assistance vs vendor responsibilities.	Implementation	Implementation Assistance	Preferred
1313	What is typical timeline to completion	What is typical timeline to complete installation?	Implementation	Implementation Assistance	Preferred
1314	Provide sample project plan, if available		Implementation	Implementation Assistance	Preferred
1315	Initial training included	Describe type of initial training provided.	Implementation	Training	Preferred
1316	Initial training included for Administrative user	Describe type of initial training provided to administrators.	Implementation	Training	Preferred
1317	Initial training included for End user	Describe type of initial training provided to end users.	Implementation	Training	Preferred
1318	Optional training available - describe.	Describe any optional training provided.	Implementation	Training	Preferred
1319	Configurations can be done by City of Surrey without vendor assistance required.		Implementation		Preferred

1320	Data conversion assistance available.		Implementation	Implementation Assistance	Preferred
1321	Additional services available - describe.	Describe any additional services available.	Implementation		Preferred
1322	Support available 24x7x365, by phone, email.		Product Support		Preferred
1323	Escalation options and procedures - describe.	Describe your escalation options and procedures.	Product Support		Preferred
1324	Post-implementation training - describe.	Describe any post-implementation training available.	Product Support	Training	Preferred
1325	Ongoing business account management process - describe.		Product Support		Preferred

TECHNICAL REQUIREMENTS					
Req. #	**Requirement**	**Elaboration**	**Category**	**Theme**	**Level of Need**
2000	Delivered as a vendor hosted Software-as-a-Service (SaaS) solution.		Infrastructure		Mandatory
2001	SaaS solution requires no additional hardware or software at City of Surrey site.		Infrastructure		Preferred
2002	System is optionally available to be fully installed at City of Surrey data center(s)		Infrastructure		Preferred
2003	System is optionally available by other means. Describe how.		Infrastructure		Preferred
2004	Multiple, redundant data centers utilized - specify certification(s).	Are multiple redundant data centers utilized? Specify certification(s).	Infrastructure	Service Recovery	Preferred
2005	Specify distance between data centers.		Infrastructure	Service Recovery	Preferred
2006	Standard maintenance window - describe.	Provide maintenance window, what is your standard?	Infrastructure	Service Recovery	Preferred

2007	Voice support for PSTN standard service - multiple telecom vendors		Infrastructure	Voice Support	Preferred
2008	Able to support VoIP (Voice Over Internet Protocol)		Infrastructure	Voice Support	Preferred
2009	Voice support capacity available	Capacity for voice support. For example; 80%, 20%	Infrastructure	Voice Support	Preferred
2010	Location of City of Surrey data.	What location is City Data stored/saved? i.e. City, Country	Infrastructure	Voice Support	Preferred
2011	Provide evidence of regular penetration tests and security audits.		Infrastructure	Security	Preferred
2012	Provide evidence of regular penetration test and security audits for Vendor internal - describe		Infrastructure	Security	Preferred
2013	Provide evidence of regular penetration test and security audits for Third party - describe		Infrastructure	Security	Preferred
2014	Provide option for City of Surrey testing/audit		Infrastructure	Security	
2015	Has established procedures and notifications for any security breach - describe.		Infrastructure	Security	Preferred
2016	Browsers supported include Internet Explorer, Chrome and Safari - describe all with supported browsers and versions.		Infrastructure	Browsers	Preferred
2017	No plug-ins required, no Active X, Flash or similar extensions required for browsers.	Does the solution have browser plug-ins or extensions?	Infrastructure	Browsers	Preferred
2018	Secure SSL connection used for browsers.		Infrastructure	Browsers	Preferred
2019	Delivery service levels provided for Voice - describe		Infrastructure	Delivery Service Level	Preferred
2020	Delivery service levels provided for SMS and email - describe		Infrastructure	Delivery Service Level	Preferred

2021	Delivery service levels provided for Email - describe		Infrastructure	Delivery Service Level	Preferred
2022	Delivery service levels provided for Pagers, other devices – describe		Infrastructure	Delivery Service Level	Preferred
2023	Email DKIM (DomainKeys Identified Mail authentication protocol) support available.		Infrastructure	Security	Preferred
2024	New releases are automatically provided		Infrastructure	New Releases	Preferred
2025	What is frequency of new releases?		Infrastructure	New Releases	Preferred
2026	Describe rollout process of new releases.		Infrastructure	New Releases	Preferred
2027	Describe cost to or action required by City of Surrey for new releases.		Infrastructure	New Releases	Preferred
2028	Web services API available for message building and sending - describe		Integration Capabilities	Web Service API	Preferred
2029	Web services API available for message results retrieval - describe		Integration Capabilities	Web Service API	Preferred
2030	Web services API available for contact and distribution list management - describe		Integration Capabilities	Web Service API	Preferred
2031	Other Web services API available - describe	Describe what other web services API's are available.	Integration Capabilities	Web Service API	Preferred
2032	Command line interface available for message sending, reporting.		Integration Capabilities	Interface	Preferred
2033	Other integration methods available – describe.	Describe what other integration methods are available.	Integration Capabilities	Interface	Preferred
2034	Contact data integrations available for HR and other internal applications/databases	Describe what integration methods are available. The City uses PeopleSoft.	Integration Capabilities	Contact Data Integrations	Preferred
2035	Contact data integrations available for BC tools – describe		Integration Capabilities	Contact Data Integrations	Preferred

2036	Other contact data integrations available - describe	Describe other contact data integrations available.	Integration Capabilities	Contact Data Integrations	Preferred
2037	Messaging integrations available for BC tools - describe	Are messaging integrations available for BC tools. Describe what integrations are available.	Integration Capabilities	Messaging Integrations	Preferred
2038	Other messaging integrations available - describe	Describe what other messaging integrations are available.	Integration Capabilities	Messaging Integrations	Preferred
2039	IT alerting integrations allow for automated triggering of messages based on events in IT tools		Integration Capabilities	IT Alerting Integrations	Preferred
2040	IT alerting integrations allow for full two-way messaging, posting results of message (who responded how) back to the IT tool		Integration Capabilities	IT Alerting Integrations	Preferred
2041	IT alerting integrations allows for assignment of the triggering issue to the "yes" responder as part of two-way messaging		Integration Capabilities	IT Alerting Integrations	Preferred
2042	IT alerting integrations available for ServiceNow - indicate if two-way		Integration Capabilities	IT Alerting Integrations	Preferred
2043	IT alerting integrations available for Microsoft SCOM – indicate if two-way		Integration Capabilities	IT Alerting Integrations	Desired
2044	Other available integrations – describe.	Describe other available IT alerting integrations.	Integration Capabilities	IT Alerting Integrations	Preferred

SERVICE LEVEL AND SUPPORT REQUIREMENTS				
Req. #	**Requirement**	**Category**	**Theme**	**Level of Need**
3000	We consider system outages as 1) a complete inability to use the solution, or 2) a reoccurring, temporary inability to use the solution, or 3) an inability to use the features and functions integral to the solution's core business purpose. Does your solution's availability criteria meet this definition? If not, please specify any departure.	Cloud	Availability	Preferred
3001	Please provide your service availability percentage (example: 99.99% Uptime). Please indicate if this percentage includes scheduled downtime. What is the frequency of measurement for service availability?	Cloud	Availability	Preferred
3002	Please indicate if the service provides geographic redundancy restricted to Canada.	Cloud	Availability	Preferred
3003	Please indicate the minimum advanced notice period you give your customers for scheduled downtime.	Cloud	Planned Maintenance	Preferred
3004	What is the estimated maximum amount of outage time required for planned maintenance? How long a service outage does your planned maintenance require for a major release?	Cloud	Planned Maintenance	Preferred
3005	Please indicate the services average latency from the south coast of BC to your services datacentre.	Cloud	Performance	Preferred
3006	Please describe your services response times.	Cloud	Performance	Preferred
3007	Please describe your service's ability to scale to meet dynamic demand loads. Please provide details about how your service scales up or down.	Cloud	Capacity	Preferred

3008	Can your service support Canadian data residency?	Cloud	Data Residency	Preferred
3009	Does your service provide the ability for the City to export City Data, either in piecemeal or in entirety, entirely at the City's discretion? If so, are there any associated costs.	Cloud	Access to City Data	Preferred
3010	Please describe your services data export capabilities, inclusive of data formats.	Cloud	Access to City Data	Preferred
3011	Does your service provide programmatic access to City Data? If so, please describe.	Cloud	Access to City Data	Preferred
3012	Does you service support data portability (the ability to move City Data to another provider at the City's discretion).	Cloud	Access to City Data	Preferred
3013	Please describe your data destruction process. Are you able to provide the City with a Certificate of Destruction that includes (any or all of): a) type of media sanitized; b) description of sanitization process and method used; c) tool used for sanitization; d) verification method; e) date of sanitization; and f) signature confirming destruction.	Cloud	Access to City Data	Preferred
3014	Please describe your change management process as it relates to service updates?	Cloud	Change Management	Preferred
3015	What is your change disclosure process and minimum notification period?	Cloud	Change Management	Preferred
3016	Does your service offer the ability to "Opt Out" of or “Roll Back” service changes?	Cloud	Change Management	Preferred
3017	Please describe your service reliability characteristics. If possible, please describe in terms of component Mean Time Between Failure (MTBF) and Mena Time to Recovery (MTTR).	Cloud	Reliability	Preferred

3018	In the event of a disaster, can your service support an RPO of 30 minutes? If not, please indicate what RPO the City can expect. Please identify if you support various tiers of DR with different RPOs, please provide details.	Cloud	Disaster Recovery	Preferred
3019	In the event of a disaster, can your service support an RTO of 1 hour? If not, please indicate what RTO the City can expect. Please identify if you support various tiers of DR with different RPOs, please provide details.	Cloud	Disaster Recovery	Preferred
3020	Please describe the process your service goes through to adequately test your fail over and disaster recovery process.	Cloud	Disaster Recovery	Preferred
3021	In the event of a disaster, does your service provide the same level of performance and availability? If not, please provide details regarding the availability and performance levels.	Cloud	Disaster Recovery	Preferred
3022	Please describe your customer/technical support model including: a) support tiers and associated incident classification levels (i.e. Critical, Major, Medium, Minor) b) response times and expected resolution times for each classification level at each tier of support c) support hours for each tier of support	Cloud	Support	Preferred
3023	For service availability percentage not met, a service credit is required. Provide details on your service credits such as how calculated, how much, when applied, process for claiming.	Cloud	Service Credit	Preferred

GENERAL SECURITY REQUIREMENTS			
Access Control			
Req. #	**Requirement**	**Category**	**Level of Need**
4000	System access must be controlled by a secure login procedure the authenticates a user's identity.	User Authentication / Secure Login	Mandatory

4001	The system must be able to leverage the City's Identity Directory (Active Directory) for user identity and authentication. This can be achieved either directly via Windows Integrated Authentication (Kerberos) or indirectly via support for SSO technologies (OpenID, OAuth, SAML, etc.) or secure LDAP.	Active Directory Integration	Mandatory
4002	The system must support roles based (or group based) access control.	Roles Based Access / Authorization	Mandatory
4003	The system must support enforcing the City's password policy. Ideally, the system can integrate with Active Directory and leverage Kerberos for authentication.	Password Management	Mandatory
4004	The system should support the use of the City's Multi-Factor authentication solution (AzureAD MFA) for access from untrusted locations.	Multi-Factor Authentication (MFA)	Preferred
4005	The system should support automatic user provisioning/de-provisioning. Note: This requirement can be ignored if AD integration is possible.	User Access Provisioning	Preferred
4006	The system should support integration with leading Privileged Identity Management solutions.	Privileged Account Management	Desired
4007	Any passwords stored in the database, the application, or configuration files must be encrypted.	Password Encryption	Mandatory

Encryption			
Req. #	**Requirement**	**Control Area**	**Level of Need**
4008	The system must support the encryption of City data while in transit.	Encryption of Data in Transit	Mandatory if Cloud, otherwise Preferred
4009	The system must support the encryption of City data while at rest.	Encryption of Data at Rest	Mandatory if Cloud, otherwise Preferred

4010	The system supports a minimum of 128-bit AES encryption using TLS 1.2 or higher for transit encryption and 256-bit AES encryption at rest. Encryption of authentication information (passwords, security questions, etc.) should use AES 128-bit encryption or SHA-2 + salt one-way hashing.	Encryption Protocols	Preferred
Auditing and Logging			
Req. #	**Requirement**	**Control Area**	**Level of Need**
4011	All security events for the system must be logged for the purpose of performing breach investigations. At a minimum, log events should be created for the following events: failed logon attempts, failed data access attempts, and system configuration changes. Log entries should include (at a minimum): UserID, Type of Event, Date/Time of Event). The system should support integration into a Security Incident and Event Management system.	Security Event Logging	Mandatory
4012	Access to log files must be controlled and only given to those individuals who have been specifically authorized (system admin, security admin, etc.). Log file should be protected from modification and deletion.	Log Protection	Preferred
4013	Systems must have the ability to produce an audit of a user's interaction with that data (viewing, modifying or deleting) in addition to producing an audit report for the security logs.	Auditing	Mandatory
Vulnerability Management			
Req. #	**Requirement**	**Control Area**	**Level of Need**
4014	System should allow for automated patch management. At the very least, security patches should be tested and then applied (automatically or manually) as soon as they are available from the vendor.	Patch Management	Preferred
4015	All systems should be able to function alongside the City's Standard Trend Miro Office Scan antivirus (this includes clients, servers, and databases). If scanning exclusions are required, they should be limited as much as possible.	Malware protection	Preferred

WEB APP SECURITY REQUIREMENTS			
Req. #	**Requirement**	**Category**	**Level of Need**
5000	Internally facing web application should have an authentication mechanism that uniquely identifies users and has a password policy which matches or improves upon the City's password policy. Externally (public) facing web-based applications should provide or support strong authentication mechanisms (multi-factor authentication).	Web Authentication	Preferred
5001	All web applications components should appropriately manage sessions to prevent session hijacking and replay. Externally facing web applications should make use of the HTTP Only flag and strict security headers.	Session Management	Preferred
5002	All web applications components should support robust roles-based access. Implementation of roles-based access is required for any web application collecting, processing, accessing or storing sensitive information.	Web Access Control	Preferred
5003	All web application components should appropriately validate input. Externally facing applications should have protections in place to prevent against the OWASP top 10, and be tested for protection against these vulnerabilities/exploits: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project	Web Input Validation	Preferred
5004	All cryptographic functions performed by the web application (or web server) should be applied on the server side and leverage the enterprise PKI (or a similar server side key management system) to manage and secure encryption keys.	Web Cryptography at Rest	Preferred
5005	All web applications should fail securely, and not reveal any sensitive or application configuration information in error messages.	Web Error Handling and Logging	Preferred
5006	All web applications should encrypt via HTTPS (TLS 1.2 or higher), and ensure no sensitive information is sent via a URL parameter. Sensitive data (PII, Credit Card Data, Financial and other sensitive City data) should never be cached client side in an unencrypted format and should be purged after a configurable period of retention.	Web Data Protection	Preferred

5007	All web services should be protected according to the OWASP Web Service Security cheat sheet: https://www.owasp.org/index.php/Web_Service_Security_Cheat_Sheet	Web Service Security	Preferred

MOBILE APP. SECURITY REQUIREMENTS			
Req. #	**Requirement**	**Category**	**Level of Need**
6000	Any sensitive data (PII, Credit Card Data, Financial and other sensitive City data) cached or stored on a mobile device must be encrypted by the mobile application. Ideally, AES 256-bit encryption is used, however, 128-bit AES or algorithms of similar (or greater) strength is sufficient. In addition, CoS must have the ability to configure a data deletion purge age (delete of X amount of time), and remotely wipe any corporate data on corporate or personal devices (corporate applications). Transmission of any sensitive data between the mobile application and a backend server must be encrypted using TLS 1.2 or higher. Corporate applications should leverage mutual authentication as part of the encryption process (server and client certs required for nailing up a TLS session).	Data Protection	Mandatory
6001	Mobile applications accessing, collecting, processing or storing sensitive data (PII, Credit Card Data, Financial and other sensitive City data) information must uniquely identify users and secure access with a strong password (8 character minimum). These passwords should not be stored on the device in any format, (even if hashed or encrypted; however, the risk is significantly less if passwords are encrypted or hashed) or viewable in any application cache or log file. Corporate application must comply with the existing password policy and must require some second factor for granting access (certificate, biometric, etc.).	Mobile Access Control	Mandatory
6002	Mobile applications should be regularly tested for vulnerabilities, either by the vendor or an internal city team. Patches should be applied as soon as they are available from the vendor and tested. Anti-malware support is required when needed (apps designed to run on Android and Windows platforms).	Mobile Vulnerability Management	Preferred

CLOUD SEC. REQUIREMENTS			
Req. #	**Requirement**	**Category**	**Level of Need**
7000	Applications and programming interfaces (APIs) should be designed, developed, deployed, and tested in accordance with leading industry standards and adhere to applicable legal, statutory, or regulatory compliance obligations.	Application & Interface Security Application Security	Preferred
7001	Prior to granting a customer access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	Application & Interface Security Customer Access Requirements	Mandatory
7002	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	Application & Interface Security Data Integrity	Preferred
7003	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity and availability) across multiple system interfaces, jurisdictions and business functions to prevent improper disclosure, alteration, or destruction.	Application & Interface Security Data Security / Integrity	Preferred
7004	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities should be agreed upon prior to executing any audits.	Audit Assurance & Compliance Audit Planning	Preferred
7005	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	Audit Assurance & Compliance Independent Audits	Mandatory
7006	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.	Audit Assurance & Compliance Information System Regulatory Mapping	Preferred

7007	A consistent unified framework for business continuity planning and plan development shall be established, documented and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval • Defined lines of communication, roles, and responsibilities • Detailed recovery procedures, manual work-around, and reference information • Method for plan invocation	Business Continuity Management & Operational Resilience Business Continuity Planning	Preferred
7008	Business continuity and security incident response plans shall be subject to testing at planned annually or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.	Business Continuity Management & Operational Resilience Business Continuity Testing	Mandatory
7009	Datacenter utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.	Business Continuity Management & Operational Resilience Datacenter Utilities / Environmental Conditions	Preferred
7010	Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system’s security features	Business Continuity Management & Operational Resilience Documentation	Preferred

7011	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.	Business Continuity Management & Operational Resilience Environmental Risks	Mandatory
7012	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.	Business Continuity Management & Operational Resilience Equipment Location	Preferred
7013	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.	Business Continuity Management & Operational Resilience Equipment Maintenance	Preferred
7014	Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific Business Impact Assessment	Business Continuity Management & Operational Resilience Equipment Power Failures	Preferred
7015	There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners, and third party service providers • Understand threats to critical products and services • Determine impacts resulting from planned or unplanned disruptions and how these vary over time • Establish the maximum tolerable period for disruption • Establish priorities for recovery • Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption • Estimate the resources required for resumption	Business Continuity Management & Operational Resilience Impact Analysis	Preferred

7016	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.	Business Continuity Management & Operational Resilience Policy	Preferred
7017	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.	Business Continuity Management & Operational Resilience Retention Policy	Preferred
7018	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or datacenter facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.	Change Control & Configuration Management New Development / Acquisition	Preferred
7019	External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g. ITIL service management processes).	Change Control & Configuration Management Outsourced Development	Preferred
7020	Organization shall follow a defined quality change control and testing process (e.g. ITIL Service Management) with established baselines, testing, and release standards that focus on system availability, confidentiality, and integrity of systems and services.	Change Control & Configuration Management Quality Testing	Preferred

7021	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to restrict the installation of unauthorized software on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Change Control & Configuration Management Unauthorized Software Installations	Preferred
7022	Policies and procedures shall be established for managing the risks associated with applying changes to: • business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations • infrastructure network and systems components Technical measures shall be implemented to provide assurance that all changes directly correspond to a registered change request, business-critical or customer (tenant) , and/or authorization by, the customer (tenant) as per agreement (SLA) prior to deployment.	Change Control & Configuration Management Production Changes	Preferred
7023	Data and objects containing data shall be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.	Data Security & Information Lifecycle Management Classification	Preferred
7024	Policies and procedures shall be established to inventory, document, and maintain data flows for data that is resident (permanently or temporarily) within the service's applications and infrastructure network and systems. In particular, providers shall ensure that data that is subject to geographic residency requirements not be migrated beyond its defined bounds.	Data Security & Information Lifecycle Management Data Inventory / Flows	Mandatory
7025	Data related to electronic commerce (e-commerce) that traverses public networks shall be appropriately classified and protected from fraudulent activity, unauthorized disclosure, or modification in such a manner to prevent contract dispute and compromise of data.	Data Security & Information Lifecycle Management eCommerce Transactions	Preferred
7026	Policies and procedures shall be established for the labeling, handling, and security of data and objects which contain data. Mechanisms for label inheritance shall be implemented for objects that act as aggregate containers for data.	Data Security & Information Lifecycle Management Handling / Labeling / Security Policy	Preferred
7027	Production City data shall not be replicated or used in non-production environment without the expressed written of the City.	Data Security & Information Lifecycle Management Non-Production Data	Mandatory

7028	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	Data Security & Information Lifecycle Management Ownership / Stewardship	Preferred
7029	Any use of City data in non-production environments requires explicit, documented approval from all customers whose data is affected, and must comply with all legal and regulatory requirements for scrubbing of sensitive data elements.	Data Security & Information Lifecycle Management Secure Disposal	Mandatory
7030	Assets should be classified in terms of business criticality, service-level expectations, and operational continuity requirements. A complete inventory of business-critical assets located at all sites and/or geographical locations and their usage over time shall be maintained and updated regularly, and assigned ownership by defined roles and responsibilities.	Datacenter Security Asset Management	Preferred
7031	Physical security perimeters (e.g., fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks, and security patrols) shall be implemented to safeguard sensitive data and information systems.	Datacenter Security Controlled Access Points	Mandatory
7032	Automated equipment identification shall be used as a method of connection authentication. Location-aware technologies may be used to validate connection authentication integrity based on known equipment location.	Datacenter Security Equipment Identification	Preferred
7033	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.	Datacenter Security Off-Site Authorization	Mandatory
7034	Policies and procedures shall be established for the secure disposal of computing equipment. This shall include a wiping solution or destruction process that renders recovery of information impossible. The erasure shall consist of a full overwrite of the drive to ensure that the erased drive is released to inventory for reuse and deployment, or securely stored until it can be destroyed.	Datacenter Security Off-Site Equipment	Preferred
7035	Policies and procedures shall be established, and supporting business processes implemented, for maintaining a safe and secure working environment in offices, rooms, facilities, and secure areas storing sensitive data (PII, Credit Card Data, Financial and other sensitive City data).	Datacenter Security Policy	Preferred
7036	Ingress and egress to secure areas shall be constrained and monitored by physical access control mechanisms to ensure that only authorized personnel are allowed access.	Datacenter Security - Secure Area Authorization	Mandatory

7037	Ingress and egress points such as service areas and other points where unauthorized personnel may enter the premises shall be monitored, controlled and, if possible, isolated from data storage and processing facilities to prevent unauthorized data corruption, compromise, and loss.	Datacenter Security Unauthorized Persons Entry	Mandatory
7038	Physical access to information assets and functions by users and support personnel shall be restricted.	Datacenter Security User Access	Mandatory
7039	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	Encryption & Key Management Entitlement	Mandatory
7040	Policies and procedures shall be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider shall inform the customer (tenant) of changes within the cryptosystem, especially if the customer (tenant) data is used as part of the service, and/or the customer (tenant) has some shared responsibility over implementation of the control.	Encryption & Key Management Key Generation	Preferred
7041	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for the use of encryption protocols for protection of sensitive data (PII, Credit Card Data, Financial and other sensitive City data) in storage (e.g., file servers, databases, and end-user workstations), data in use (memory), and data in transmission (e.g., system interfaces, over public networks, and electronic messaging) as per applicable legal, statutory, and regulatory compliance obligations.	Encryption & Key Management Sensitive Data Protection	Mandatory
7042	Platform and data-appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms shall be required. Keys shall not be stored in the cloud (i.e. at the cloud provider in question), but maintained by the cloud consumer or trusted key management provider. Key management and key usage shall be separated duties.	Encryption & Key Management Storage and Access	Preferred

7043	Baseline security requirements shall be established for developed or acquired, organizationally-owned or managed, physical or virtual, applications and infrastructure system and network components that comply with applicable legal, statutory and regulatory compliance obligations. Deviations from standard baseline configurations should be authorized following change management policies and procedures prior to deployment, provisioning, or use. Compliance with security baseline requirements should be reassessed at least annually unless an alternate frequency has been established and authorized based on business need.	Governance and Risk Management Baseline Requirements	Preferred
7044	Risk assessments associated with data governance requirements shall be conducted at planned intervals and shall consider the following: • Awareness of where sensitive data is stored and transmitted across applications, databases, servers, and network infrastructure • Compliance with defined retention periods and end-of-life disposal requirements • Data classification and protection from unauthorized use, access, loss, destruction, and falsification	Governance and Risk Management Data Focus Risk Assessments	Preferred
7045	Cloud provider managers are responsible for maintaining awareness of, and complying with, security policies, procedures, and standards that are relevant to their area of responsibility.	Governance and Risk Management Management Oversight	Preferred
7046	An Information Security Management Program (ISMP) shall be developed, documented, approved, and implemented by the Cloud Provider that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program shall include, but not be limited to, the following areas insofar as they relate to the characteristics of the business: • Risk management • Security policy • Organization of information security • Asset management • Human resources security • Physical and environmental security • Communications and operations management • Access control • Information systems acquisition, development, and maintenance	Governance and Risk Management Management Program	Mandatory

7047	Executive and line management shall take formal action to support information security through clearly-documented direction and commitment, and shall ensure the action has been assigned.	Governance and Risk Management Management Support/Involvement	Preferred
7048	Information security policies and procedures shall be established and made readily available for review by all impacted personnel and external business relationships. Information security policies should be authorized by the organization's business leadership (or other accountable business role or function) and supported by a strategic business plan and an information security management program inclusive of defined information security roles and responsibilities for business leadership.	Governance and Risk Management Policy	Preferred
7049	A formal disciplinary or sanction policy shall be established for employees who have violated security policies and procedures. Employees shall be made aware of what action might be taken in the event of a violation, and disciplinary measures should be stated in the policies and procedures.	Governance and Risk Management Policy Enforcement	Preferred
7050	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	Governance and Risk Management Policy Impact on Risk Assessments	Preferred
7051	The organization's business leadership (or other accountable business role or function) shall review the information security policy at planned intervals or as a result of changes to the organization to ensure its continuing alignment with the security strategy, effectiveness, accuracy, relevance, and applicability to legal, statutory, or regulatory compliance obligations.	Governance and Risk Management Policy Reviews	Preferred
7052	Aligned with the enterprise-wide framework, formal risk assessments shall be performed at least annually or at planned intervals, (and in conjunction with any changes to information systems) to determine the likelihood and impact of all identified risks using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk shall be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).	Governance and Risk Management Risk Assessments	Preferred
7053	Risks shall be mitigated to an acceptable level. Acceptance levels based on risk criteria shall be established and documented in accordance with reasonable resolution time frames and stakeholder approval.	Governance and Risk Management Risk Management Framework	Mandatory

7054	Upon termination of the Cloud Provider's workforce personnel and/or expiration of external business relationships, all Cloud Provider-owned assets and data (including any copies of data) shall be returned within an established period.	Human Resources Asset Returns	Preferred
7055	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties shall be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.	Human Resources Background Screening	Preferred
7056	Employment agreements shall incorporate provisions and/or terms for adherence to established information governance and security policies and must be signed by newly hired or on-boarded workforce personnel (e.g., full or part-time employee or contingent staff) prior to granting workforce personnel user access to corporate facilities, resources, and assets.	Human Resources Employment Agreements	Preferred
7057	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.	Human Resources Employment Termination	Preferred
7058	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to manage business risks associated with permitting mobile device access to corporate resources and may require the implementation of higher assurance compensating controls and acceptable-use policies and procedures (e.g., mandated security training, stronger identity, entitlement and access controls, and device monitoring).	Human Resources Mobile Device Management	Preferred
7059	Requirements for non-disclosure or confidentiality agreements reflecting the organization's needs for the protection of data and operational details shall be identified, documented, and reviewed annually.	Human Resources Non-Disclosure Agreements	Mandatory
7060	Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.	Human Resources Roles / Responsibilities	Mandatory

7061	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining allowances and conditions for permitting usage of organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components. Additionally, defining allowances and conditions to permit usage of personal mobile devices and associated applications with access to corporate resources (i.e., BYOD) shall be considered and incorporated as appropriate.	Human Resources Technology Acceptable Use	Preferred
7062	A security awareness training program shall be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data shall receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	Human Resources Training / Awareness	Preferred
7063	All personnel shall be made aware of their roles and responsibilities for: • Maintaining awareness and compliance with established policies and procedures and applicable legal, statutory, or regulatory compliance obligations. • Maintaining a safe and secure working environment	Human Resources User Responsibility	Preferred
7064	Policies and procedures shall be established to require that unattended workspaces do not have openly visible (e.g., on a desktop) sensitive documents and user computing sessions are disabled after an established period of inactivity.	Human Resources Workspace	Preferred
7065	Access to, and use of, audit tools that interact with the organization's information systems shall be appropriately segmented and restricted to prevent compromise and misuse of log data.	Identity & Access Management Audit Tools Access	Mandatory

7066	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally-owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures should incorporate the following: • Procedures and supporting roles and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)) • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-factor, expireable, non-shared authentication secrets) • Permissions and supporting capabilities for customer (tenant) controls over authentication, authorization, and accounting (AAA) rules for access to data and sessions • Adherence to applicable legal, statutory, or regulatory compliance requirements	Identity & Access Management Credential Lifecycle / Provision Management	Preferred

7067	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	Identity & Access Management Diagnostic / Configuration Ports Access	Preferred
7068	Policies and procedures shall be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies shall also be developed to control access to network resources based on user identity.	Identity & Access Management Policies and Procedures	Preferred
7069	User access policies and procedures shall be established, and supporting business processes and technical measures implemented, for restricting user access as per defined segregation of duties to address business risks associated with a user-role conflict of interest.	Identity & Access Management Segregation of Duties	Preferred
7070	Access to the organization's own developed applications, program, or object source code, or any other form of intellectual property (IP), and use of proprietary software shall be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.	Identity & Access Management Source Code Access Restriction	Preferred
7071	The identification, assessment, and prioritization of risks posed by business processes requiring third-party access to the organization's information systems and data shall be followed by coordinated application of resources to minimize, monitor, and measure likelihood and impact of unauthorized or inappropriate access. Compensating controls derived from the risk analysis shall be implemented prior to provisioning access.	Identity & Access Management Third Party Access	Mandatory
7072	Policies and procedures are established for permissible storage and access of identities used for authentication to ensure identities are only accessible based on rules of least privilege and replication limitation only to users explicitly defined as business necessary.	Identity & Access Management Trusted Sources	Preferred

7073	Provisioning user access (e.g., employees, contractors, customers (tenants), business partners and/or supplier relationships) to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components shall be authorized by the organization's management prior to access being granted and appropriately restricted as per established policies and procedures. Upon request, provider shall inform customer (tenant) of this user access, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Identity & Access Management User Access Authorization	Mandatory
7074	User access shall be authorized and revalidated for entitlement appropriateness, at planned intervals, by the organization's business leadership or other accountable business role or function supported by evidence to demonstrate the organization is adhering to the rule of least privilege based on job function. For identified access violations, remediation must follow established user access policies and procedures.	Identity & Access Management User Access Reviews	Mandatory
7075	Timely de-provisioning (revocation or modification) of user access to data and organizationally-owned or managed (physical and virtual) applications, infrastructure systems, and network components, shall be implemented as per established policies and procedures and based on user's change in status (e.g., termination of employment or other business relationship, job change or transfer). Upon request, provider shall inform customer (tenant) of these changes, especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Identity & Access Management User Access Revocation	Mandatory

7076	Internal corporate or customer (tenant) user account credentials shall be restricted as per the following, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures: • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expireable, non-shared authentication secrets)	Identity & Access Management User ID Credentials	Preferred
7077	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.	Identity & Access Management Utility Programs Access	Mandatory
7078	Higher levels of assurance are required for protection, retention, and lifecycle management of audit logs, adhering to applicable legal, statutory or regulatory compliance obligations and providing unique user access accountability to detect potentially suspicious network behaviors and/or file integrity anomalies, and to support forensic investigative capabilities in the event of a security breach.	Infrastructure & Virtualization Security Audit Logging / Intrusion Detection	Mandatory
7079	The provider shall ensure the integrity of all virtual machine images at all times. Any changes made to virtual machine images must be logged and an alert raised regardless of their running state (e.g. dormant, off, or running). The results of a change or move of an image and the subsequent validation of the image's integrity must be immediately available to customers through electronic methods (e.g. portals or alerts).	Infrastructure & Virtualization Security Change Detection	Mandatory
7080	A reliable and mutually agreed upon external time source shall be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.	Infrastructure & Virtualization Security Clock Synchronization	Preferred
7081	The availability, quality, and adequate capacity and resources shall be planned, prepared, and measured to deliver the required system performance in accordance with legal, statutory, and regulatory compliance obligations. Projections of future capacity requirements shall be made to mitigate the risk of system overload.	Infrastructure & Virtualization Security Information System Documentation	Preferred

7082	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g. virtualization aware).	Infrastructure & Virtualization Security Management - Vulnerability Management	Mandatory
7083	Network environments and virtual instances shall be designed and configured to restrict and monitor traffic between trusted and untrusted connections. These configurations shall be reviewed at least annually, and supported by a documented justification for use for all allowed services, protocols, and ports, and by compensating controls.	Infrastructure & Virtualization Security Network Security	Mandatory
7084	Each operating system shall be hardened to provide only necessary ports, protocols, and services to meet business needs and have in place supporting technical controls such as: antivirus, file integrity monitoring, and logging as part of their baseline operating build standard or template.	Infrastructure & Virtualization Security OS Hardening and Base Controls	Mandatory
7085	Production and non-production environments shall be separated to prevent unauthorized access or changes to information assets. Separation of the environments may include: stateful inspection firewalls, domain/realm authentication sources, and clear segregation of duties for personnel accessing these environments as part of their job duties.	Infrastructure & Virtualization Security Production / Non-Production Environments	Mandatory
7086	Multi-tenant organizationally-owned or managed (physical and virtual) applications, and infrastructure system and network components, shall be designed, developed, deployed and configured such that provider and City (tenant) user access is appropriately segmented from other customer/tenant users, based on the following considerations: • Established policies and procedures • Isolation of business critical assets and/or sensitive data (PII, Credit Card Data, Financial and other sensitive City data), and sessions that mandate stronger internal controls and high levels of assurance • Compliance with legal, statutory and regulatory compliance obligations	Infrastructure & Virtualization Security Segmentation	Mandatory
7087	Secured and encrypted communication channels shall be used when migrating physical servers, applications, or data to virtualized servers and, where possible, shall use a network segregated from production-level networks for such migrations.	Infrastructure & Virtualization Security VM Security - vMotion Data Protection	Mandatory

7088	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).	Infrastructure & Virtualization Security VMM Security - Hypervisor Hardening	Mandatory
7089	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to protect wireless network environments, including the following: • Perimeter firewalls implemented and configured to restrict unauthorized traffic • Security settings enabled with strong encryption for authentication and transmission, replacing vendor default settings (e.g., encryption keys, passwords, and SNMP community strings) • User access to wireless network devices restricted to authorized personnel • The capability to detect the presence of unauthorized (rogue) wireless network devices for a timely disconnect from the network	Infrastructure & Virtualization Security Wireless Security	Mandatory
7090	Network architecture diagrams shall clearly identify high-risk environments and data flows that may have legal compliance impacts. Technical measures shall be implemented and shall apply defense-in-depth techniques (e.g., deep packet analysis, traffic throttling, and black-holing) for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns (e.g., MAC spoofing and ARP poisoning attacks) and/or distributed denial-of-service (DDoS) attacks.	Infrastructure & Virtualization Security Network Architecture	Mandatory
7091	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	Interoperability & Portability APIs	Preferred
7092	All structured and unstructured data shall be available to the customer and provided to them upon request in an industry-standard format (e.g., .doc, .xls, .pdf, logs, and flat files)	Interoperability & Portability Data Request	Mandatory

7093	Policies, procedures, and mutually-agreed upon provisions and/or terms shall be established to satisfy customer (tenant) requirements for service-to-service application (API) and information processing interoperability, and portability for application development and information exchange, usage, and integrity persistence.	Interoperability & Portability Policy & Legal	Preferred
7094	The provider shall use secure (e.g., non-clear text and authenticated) standardized network protocols for the import and export of data and to manage the service, and shall make available a document to consumers (tenants) detailing the relevant interoperability and portability standards that are involved.	Interoperability & Portability Standardized Network Protocols	Mandatory
7095	The provider shall use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and shall have documented custom changes made to any hypervisor in use and all solution-specific virtualization hooks available for customer review.	Interoperability & Portability Virtualization	Preferred
7096	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.	Mobile Security Anti-Malware	Preferred
7097	A documented list of approved application stores has been defined as acceptable for mobile devices accessing or storing provider managed data.	Mobile Security Application Stores	Preferred
7098	The company shall have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.	Mobile Security Approved Applications	Preferred
7099	The BYOD policy and supporting awareness training clearly states the approved applications, application stores, and application extensions and plugins that may be used for BYOD usage.	Mobile Security Approved Software for BYOD	Preferred
7100	The provider shall have a documented mobile device policy that includes a documented definition for mobile devices and the acceptable usage and requirements for all mobile devices. The provider shall post and communicate the policy and requirements through the company's security awareness and training program.	Mobile Security Awareness and Training	Preferred
7101	All cloud-based services used by the company's mobile devices or BYOD shall be pre-approved for usage and the storage of company business data.	Mobile Security Cloud Based Services	Mandatory

7102	The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.	Mobile Security Compatibility	Preferred
7103	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.	Mobile Security Device Eligibility	Preferred
7104	An inventory of all mobile devices used to store and access company data shall be kept and maintained. All changes to the status of these devices (i.e., operating system and patch levels, lost or decommissioned status, and to whom the device is assigned or approved for usage (BYOD)) will be included for each device in the inventory.	Mobile Security Device Inventory	Mandatory
7105	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.	Mobile Security Device Management	Mandatory
7106	The mobile device policy shall require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and shall be enforced through technology controls.	Mobile Security Encryption	Preferred
7107	The mobile device policy shall prohibit the circumvention of built-in security controls on mobile devices (e.g. jailbreaking or rooting) and shall enforce the prohibition through detective and preventative controls on the device or through a centralized device management system (e.g. mobile device management).	Mobile Security Jailbreaking and Rooting	Preferred
7108	The BYOD policy includes clarifying language for the expectation of privacy, requirements for litigation, e-discovery, and legal holds. The BYOD policy shall clearly state the expectations regarding the loss of non-company data in the case a wipe of the device is required.	Mobile Security Legal	Preferred
7109	BYOD and/or company-owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.	Mobile Security Lockout Screen	Mandatory
7110	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.	Mobile Security Operating Systems	Preferred
7111	Password policies, applicable to mobile devices, shall be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and shall prohibit the changing of password/PIN lengths and authentication requirements.	Mobile Security Passwords	Preferred

7112	The mobile device policy shall require the BYOD user to perform backups of data, prohibit the usage of unapproved application stores, and require the use of anti-malware software (where supported).	Mobile Security Policy	Preferred
7113	All mobile devices permitted for use through the company BYOD program or a company-assigned mobile device shall allow for remote wipe by the company's corporate IT or shall have all company-provided data wiped by the company's corporate IT.	Mobile Security Remote Wipe	Preferred
7114	Mobile devices connecting to corporate networks, or storing and accessing company information, shall allow for remote software version/patch validation. All mobile devices shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier and authorized IT personnel shall be able to perform these updates remotely.	Mobile Security Security Patches	Mandatory
7115	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.	Mobile Security Users	Preferred
7116	Points of contact for applicable regulation authorities, national and local law enforcement, and other legal jurisdictional authorities shall be maintained and regularly updated (e.g., change in impacted-scope and/or a change in any compliance obligation) to ensure direct compliance liaisons have been established and to be prepared for a forensic investigation requiring rapid engagement with law enforcement.	Security Incident Management, E-Discovery & Cloud Forensics Contact / Authority Maintenance	Mandatory
7117	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to triage security-related events and ensure timely and thorough incident management, as per established IT service management policies and procedures.	Security Incident Management, E-Discovery & Cloud Forensics Incident Management	Preferred
7118	Workforce personnel and external business relationships shall be informed of their responsibilities and, if required, shall consent and/or contractually agree to report all information security events in a timely manner. Information security events shall be reported through predefined communications channels in a timely manner adhering to applicable legal, statutory, or regulatory compliance obligations.	Security Incident Management, E-Discovery & Cloud Forensics Incident Reporting	Mandatory

7119	Proper forensic procedures, including chain of custody, are required for the presentation of evidence to support potential legal action subject to the relevant jurisdiction after an information security incident. Upon notification, customers and/or other external business partners impacted by a security breach shall be given the opportunity to participate as is legally permissible in the forensic investigation.	Security Incident Management, E-Discovery & Cloud Forensics Incident Response Legal Preparation	Mandatory
7120	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	Security Incident Management, E-Discovery & Cloud Forensics Incident Response Metrics	Preferred
7121	Providers shall inspect, account for, and work with their cloud supply-chain partners to correct data quality errors and associated risks. Providers shall design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain.	Supply Chain Management, Transparency and Accountability Data Quality and Integrity	Mandatory
7122	The provider shall make security incident information available to the City and providers periodically through electronic methods (e.g. portals).	Supply Chain Management, Transparency and Accountability Incident Reporting	Mandatory
7123	Business-critical or customer (tenant) impacting (physical and virtual) application and system-system interface (API) designs and configurations, and infrastructure network and systems components, shall be designed, developed, and deployed in accordance with mutually agreed-upon service and capacity-level expectations, as well as IT governance and service management policies and procedures.	Supply Chain Management, Transparency and Accountability Network / Infrastructure Services	Preferred
7124	The provider shall perform annual internal assessments of conformance to, and effectiveness of, its policies, procedures, and supporting measures and metrics.	Supply Chain Management, Transparency and Accountability Provider Internal Assessments	Mandatory

7125	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) shall incorporate at least the following mutually-agreed upon provisions and/or terms: • Scope of business relationship and services offered (e.g., customer (tenant) data acquisition, exchange and usage, feature sets and functionality, personnel and infrastructure network and systems components for service delivery and support, roles and responsibilities of provider and customer (tenant) and any subcontracted or outsourced business relationships, physical geographical location of hosted services, and any known regulatory compliance considerations) • Information security requirements, provider and customer (tenant) primary points of contact for the duration of the business relationship, and references to detailed supporting and relevant business processes and technical measures implemented to enable effectively governance, risk management, assurance and legal, statutory and regulatory compliance obligations by all impacted business relationships • Notification and/or pre-authorization of any changes controlled by the provider with customer (tenant) impacts • Timely notification of a security incident (or confirmed breach) to all customers (tenants) and other business relationships impacted (i.e., up- and down-stream impacted supply chain) • Assessment and independent verification of compliance with agreement provisions and/or terms (e.g., industry-acceptable certification, attestation audit report, or equivalent forms of assurance) without posing an unacceptable business risk of exposure to the organization being assessed • Expiration of the business relationship and treatment of customer (tenant) data impacted • Customer (tenant) service-to-service application (API) and data interoperability and portability requirements for application development and information exchange, usage, and integrity persistence	Supply Chain Management, Transparency and Accountability Supply Chain Agreements	Preferred
7126	Providers shall review the risk management and governance processes of their partners so that practices are consistent and aligned to account for risks inherited from other members of that partner's cloud supply chain.	Supply Chain Management, Transparency and Accountability Supply Chain Governance Reviews	Preferred

7127	Policies and procedures shall be implemented to ensure the consistent review of service agreements (e.g., SLAs) between providers and customers (tenants) across the relevant supply chain (upstream/downstream). Reviews shall performed at least annually and identity non-conformance to established agreements. The reviews should result in actions to address service-level conflicts or inconsistencies resulting from disparate supplier relationships.	Supply Chain Management, Transparency and Accountability Supply Chain Metrics	Preferred
7128	Providers shall assure reasonable information security across their information supply chain by performing an annual review. The review shall include all partners/third party-providers upon which their information supply chain depends on.	Supply Chain Management, Transparency and Accountability Third Party Assessment	Mandatory
7129	Third-party service providers shall demonstrate compliance with information security and confidentiality, access control, service definitions, and delivery level agreements included in third-party contracts. Third-party reports, records, and services shall undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.	Supply Chain Management, Transparency and Accountability Third Party Audits	Preferred
7130	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of malware on organizationally-owned or managed user end-point devices (i.e., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Threat and Vulnerability Management Anti-Virus / Malicious Software	Preferred

7131	Policies and procedures shall be established, and supporting processes and technical measures implemented, for timely detection of vulnerabilities within organizationally-owned or managed applications, infrastructure network and system components (e.g. network vulnerability assessment, penetration testing) to ensure the efficiency of implemented security controls. A risk-based model for prioritizing remediation of identified vulnerabilities shall be used. Changes shall be managed through a change management process for all vendor-supplied patches, configuration changes, or changes to the organization's internally developed software. Upon request, the provider informs the City (tenant) of policies and procedures and identified weaknesses especially if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Threat and Vulnerability Management Vulnerability / Patch Management	Mandatory
7132	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to prevent the execution of unauthorized mobile code, defined as software transferred between systems over a trusted or untrusted network and executed on a local system without explicit installation or execution by the recipient, on organizationally-owned or managed user end-point devices (e.g., issued workstations, laptops, and mobile devices) and IT infrastructure network and systems components.	Threat and Vulnerability Management Mobile Code	Preferred

SCHEDULE B – ATTACHMENT 1

CLOUD SERVICES IMPLEMENTATION, SUBSCRIPTION, AND SERVICE LEVEL AGREEMENT

Title: **EMERGENCY NOTIFICATION SOFTWARE**

Reference No.: **1220-040-2019-095**

FOR THE SUPPLY OF GOODS AND SERVICES

(GENERAL SERVICES)

TABLE OF CONTENTS

CLOUD SERVICES AGREEMENT IMPLEMENTATION

DRAFT AGREEMENT – CLOUD SERVICES IMPLEMENTATION, SUBSCRIPTION, AND SERVICE LEVEL AGREEMENT

SUPPLY & IMPLEMENTATION OF EMERGENCY NOTIFICATION SOFTWARE

This Agreement is effective this _____ day of _____, 2019.

AGREEMENT #1220-040-2019-095

BETWEEN:

CITY OF SURREY
13450 - 104th Avenue
Surrey, British Columbia, Canada, V3T 1V8

(the "**City**")

OF THE FIRST PART

AND:

(Insert Full Legal Name/Address of Contractor)
(the "**Contractor**")

OF THE SECOND PART

WHEREAS:

A. The Contractor has developed and owns the copyright and all other proprietary rights pertaining to and subsisting in certain computer programs as a hosted service, including related documentation, (the "Cloud Services") generally as set out in Appendix 1 – Scope of Services;

B. The City requires for its business operations that the Cloud Services functions to the standard set out in Appendix 8 – Service Level Agreement;

C. The Contractor has experience implementing the Cloud Services and is able to complete integrations, interfaces and customizations (the "Professional Services") generally as set out in Appendix 1 – Scope of Services;

D. The Contractor desires to make the Cloud Services available to the City and the City desires to acquire access to the Cloud Services from the Contractor; and

E. The Contractor desires to provide the Implementation Services for the City and the City desires to have the Implementation Services provided by the Contractor.

THEREFORE in consideration of the payment of one ($1.00) dollar and other good and valuable consideration paid by each of the parties to the other (the receipt and sufficiency of which is hereby acknowledged) the City and the Contractor agree as follows:

1. INTERPRETATION

1.1 Definitions

In this Agreement the following definitions apply:

"Agreement" means this Cloud Services Implementation, License, and Service Level Agreement between the City and Contractor, inclusive of all schedules, attachments, addenda and other documents incorporated by reference;

"**Change**" means an addition to, deletion from or alteration of the Services, as agreed to by the parties in accordance with Section 2.2;

"**Change Order**" has the meaning set out in Section 2.2;

"**City Data**" means all information, in writing (including electronic) form, created by or in any way originating with City, and all information that is the output of any computer processing, or other electronic manipulation, of any information that was created by or in any way originating with City, in the course of using and configuring the Services provided under this Agreement, that is stored on the SaaS;

"**City Representative**" (or designate) who will have the duty of instituting and maintaining communication with the Contractor as to the requirements of the Agreement including but not limited to receive security incident or breach notification;

"**Cloud Services**", which may encompass software-as-a-service, platform-as-a-service, and infrastructure-as-a-service, has the meaning set out in Appendix A – Scope of Services;

"**Confidential Information**" means information supplied to, obtained by, or which comes to the knowledge of the Contractor and the City (or either of them) as a result of the performance of the Services and this Agreement, which includes, but is not limited to, Personal Information, information that relates to the business of the third party, and information that is subject to solicitor-client privilege;

"**Contemplated Change Order**" has the meaning set out in Section 2.2.2;

"**Data Breach**" means any actual or reasonably suspected unauthorized access to or acquisition of Data;

"**Dispute**" has the meaning set out in Section 26.1;

"**Documentation"** has the meaning set out in Section 2.4;

"**Effective Date**" means the date when this Agreement has been fully executed by both parties' authorized signatories;

"**Enhancements**" means any improvements, modifications, upgrades, updates, fixes, revisions and/or expansions to the Services that Contractor may develop or acquire and

incorporate into its standard version of the Services or which the Contractor has elected to make generally available to its customers;

"**Fees**" has the meaning set out in Section 7.1;

"**Go-Live Date**" means the date on which the City, acting reasonably, confirms that the Cloud Services satisfy the functional and technical requirements as set out in this Agreement;

"**Indemnitees**" has the meaning set out in Section 10.1;

"**Intellectual Property Rights**" has the meaning set out in Section 9;

"**Invoice**" has the meaning set out in Section 7.2.1;

"**License Costs**" shall mean the reoccurring fee paid to the Contractor as compensation for continued use of the Cloud Services;

"**Marks**" has the meaning set out in Section 2.5;

"**Performance Report**" has the meaning set out in Section 2.10.1;

"**Personal Information**" means information about an identifiable individual and any other types of information that, alone or in combination, would reveal the identity of a particular individual, other than business contact information;

"**Quotation**" has the meaning set out in Section 2.2.3;

"**Renewal Term**" has the meaning set out in Article 4;

"**Security Incident**" means any actual or reasonably suspected adverse event that compromises the availability, confidentiality, or integrity of the Data, or the ability of the City to access the Data;

"**Services**" means all services required to be performed by the Contractor under this Agreement, including but not limited to the Cloud Services and any Professional Services;

"**Services Expansion**" has the meaning set out in Section 2.11.1;

"**Source Code**" means a set of instructions, written in programming language, that must be translated to machine instructions before the program can run on a computer. These instructions must be compiled into object code before the computer can understand them;

"**Subscription Fee**" shall mean the reoccurring fee paid to the Contractor as compensation for continued use of the Cloud Services;

"**Term**" means the Initial Term and, as applicable, the First Renewal Term and the Second Renewal Term and the Third Renewal Term, all as described in Article 4; and

"**Third Party**" means persons, corporations and entities other than Contractor, City or any of their employees, or agents.

1.2 Appendices

1.2.1 The following attached Appendices are a part of this Agreement:

(a) Appendix 1 – Scope of Services;
(b) Appendix 1-A – Functional and Technical Requirements;
(c) Appendix 2 – Fees and Payment;
(d) Appendix 3 – Time Schedule;
(e) Appendix 4 – Key Personnel and Sub-Contractors;
(f) Appendix 5 – Professional Services;
(g) Appendix 6 – Privacy Protection Schedule;
(h) Appendix 7 – Confidentiality Agreement; and
(i) Appendix 8 – Service Level Agreement.

1.2.2 This Agreement may only be modified by express and specific written agreement. In the event of a conflict between the provisions of any document listed below, then the documents shall govern and take precedence in the following order:

(a) Change orders and any written amendments to this Agreement mutually agreed upon by the parties;
(b) This Agreement;
(c) Technical specifications produced as part of the Implementation; and
(d) The RFQ and the Contractor's RFQ Response.

2. SERVICES

2.1 Services

2.1.1 This Agreement sets forth the terms and conditions under which the Contractor agrees to license certain hosted Cloud Services and provide all other services, data import / export, monitoring, support, backup and recovery, and training necessary for City's productive use of such software, as further set forth in Appendix 1, attached. The City shall perform its responsibilities set forth in the same Appendix 1. Contractor agrees to work with the City to ensure proper change management and assist in identifying any required technology upgrades within the City's network in support of this implementation. Contractor and the City shall use commercially reasonable efforts to fulfill their respective obligations in a timely manner in order to achieve the agreed milestones and dates set forth in this Agreement.

Authorized Users. Unless otherwise limited in Appendix 1, City and any of its employees, agents, contractors, suppliers of services or other designated users that have a need to use the Cloud Services for the benefit of the City shall have the right to operate and use the same. Contractor shall issue accounts, or permit the City to issue accounts, to individuals selected by City as account-holders for using the Cloud Services. Only account-holders may access or use the Cloud Services and each account-holder's access to the Cloud Services requires valid login credentials, including at least user identification and secure passwords (each an "Account"). The rights of an account-holder may not be

used by more than one individual, unless the Account of the account-holder is reassigned in its entirety to another account-holder, in which case the prior holder of the Account shall no longer have any right to access or use the Cloud Services. City acknowledges and agrees that City:

(i) is fully responsible for Accounts assigned by or at the request of the City and the acts and omissions of each account-holder, including the creation of Account credentials by any person, the maintenance, confidentiality and security of all passwords related to Accounts, and any and all activities that occur under Accounts assigned by or at request of the City.

(ii) shall notify Contractor as soon as practicable after obtaining or receiving any knowledge of (A) any unauthorized use of an Account or any password related to an Account, or (B) any other breach of security with respect to an Account, provided that such notification will not negate the City's liability for any unauthorized use of an Account or password until such time as Contractor can be reasonably expected to take corrective measures; and

(iii) will provide true, current, accurate and complete information as prompted by the Account-creation process or as otherwise requested by Contractor from time-to-time and to promptly update such information when any changes occur.

City shall:

(iv) be responsible for Account-holders' compliance with all of the terms and conditions of this Agreement;

(v) be solely responsible for the accuracy, quality, integrity and legality of any City Data the City stores on or uploads to the Cloud Services, and of the means by which City Data is acquired and used, including compliance with all personal information privacy laws and regulations and ensuring that no third party intellectual property rights are infringed; and

(vi) use all commercially reasonable efforts to prevent unauthorized access to or use of the Cloud Services, and notify Contractor promptly of any such unauthorized access or use.

The City shall not:

(vii) make the Cloud Services available to anyone, or permit anyone to access the Cloud Services, other than account-holders;

(viii) license, sublicense, sell, resell, transfer, assign, distribute, rent, lease or time-share the rights granted to City under this Agreement to use the Cloud Services, or copy or otherwise commercially exploit the Cloud

Services or its components in any way except in accordance with the rights granted hereunder;

(ix) use the Cloud Services in any manner or for any purpose (A) that contravenes, facilitates the violation of, or violates any applicable laws; (B) that extracts, gathers, collects, or stores personal information about individuals except in compliance with all applicable personal information privacy laws or that involves data mining, robots or similar data gathering or extraction methods on individual's personal information without their express consent, or (C) that interferes with or disrupts the integrity or performance of the Cloud Services;

(x) attempt to gain unauthorized access to the Cloud Services or its related systems or networks;

(xi) post, upload, reproduce, distribute or otherwise transmit on the Cloud Services (A) defamatory, infringing, indecent or unlawful software, materials or information, or (B) inappropriate, profane, or obscene software, materials or information without suitable or lawfully-required access controls;

(xii) disable or circumvent any access control or related process or procedure established with respect to the Cloud Services; or

(xiii) remove any copyright or other proprietary or intellectual property rights notices or labels on or in the Cloud Services or any part, copy or report generated therefrom or thereof.

The City acknowledges that the Cloud Services is not intended to be use as a repository of large media files. The City agrees to use the Cloud Services only for its intended purposes and not for storing large media file, failing which the Contractor may establish and enforce a reasonable limit on the size of City Data that may be stored on the Cloud Services.

2.1.2 Non-exclusivity. Nothing herein shall be deemed to preclude the City from retaining the services of other persons or entities undertaking the same or similar functions as those undertaken by Contractor hereunder.

2.2 Changes

2.2.1 The City may without invalidating this Contract make a Change to the Services. If the City makes a Change to the Services, then the Department Representative, or, designate shall issue a Change Order.

2.2.2 The Department Representative, or designate may at any time give the Contractor a written request (a "Contemplated Change Order") to provide a Quotation for a specified Change that the City is considering.

2.2.3 If the Department Representative, or designate gives the Contractor a Contemplated Change Order, then the Contractor shall, as part of the Services, respond as promptly as possible with a written price quotation (a "Quotation"). The Quotation shall comply with the following:

(a) Any Quotation submitted by the Contractor for a Change or a Contemplated Change Order shall, unless expressly stated otherwise in the Quotation, be interpreted to represent the total adjustment to the Contract Price (excluding GST) owing on account for the Services contemplated by the Quotation and for certainty shall be interpreted to include compensation on account of all related costs, including but not limited to all direct, indirect, or impact, head office, overhead, and all other costs, and all markups and profits, even if the Quotation does not specifically mention such items.

2.2.4 The Department Representative, or designate may at any time, by way of a Change Order, direct the Contractor to proceed with a Change and the Contractor shall comply with such direction.

2.2.5 The Contractor shall not proceed with any Services that the Contractor intends or expects to be treated as a Change without receiving a written Change Order approving the Services as a Change.

2.2.6 If for any reason the Contractor proceeds with Services that the Contractor intends to claim as a Change before a written Change Order is issued, then verbal approval must have been received and a written Change Order pending. The Contractor shall maintain daily records, and submit them before the end of the next day to the Department Representative, or, designate for certification. Notwithstanding any other provision of the Contract Documents, no payment shall be owing to the Contractor on account of any claimed Change if the Contractor fails to maintain and submit such records. However, the mere maintenance and submission of such daily records shall not create an entitlement for the Contractor to receive payment for the claimed Change and the Contractor's right to receive payment shall be as otherwise provided by the Contract Documents.

2.2.7 The Contractor shall not be entitled to rely on any oral representation (except in an emergency), site meeting discussion, site meeting minutes or other communication as approval that any Services are a Change. The Contractor shall strictly comply with the requirements of this section.

2.2.8 In an emergency, when it is impractical to delay the Services until the written authorization is issued, the Department Representative, or designate may issue an oral direction which the Contractor shall follow. In such event the Department Representative, or, designate shall issue a confirming Change Order at the first opportunity.

2.2.9 If Contractor eliminates any functionality of any of the Services provided under this Agreement and subsequently offers that functionality in other or new products (whether directly or indirectly through agreement with a Third Party), then the portion of those other or new products that contain the functions in question, or the entire product if the functions cannot be separated out, shall be provided to City at no additional charge and under the terms of this Agreement, including technical support. If Contractor incorporates the functionality of the Services provided under this Agreement into a newer product and

continues to offer both products, City may, in its sole discretion, exercise the option to upgrade to the newer product at no additional cost.

2.3 Standard of Care

2.3.1 The Contractor will perform the Services with that degree of care, skill and diligence normally provided by a qualified and experienced practitioner performing Services similar to the Services, and on the understanding that the City is relying on the Contractor's experience and expertise. The Contractor represents that it has the expertise, qualifications, resources and relevant experience to provide the Goods and Services.

2.4 Documentation

2.4.1 Documentation shall mean, collectively: (a) this Agreement including any amendment thereto; (b) all materials published or otherwise made available to City by the Contractor that relate to the functional, operational and/or performance capabilities of the Cloud Services; (c) all user, operator, system administration, technical, support and other manuals and all other materials published or otherwise made available by the Contractor that describe the functional, operational and/or performance capabilities of the Cloud Services; (d) any Requests for Information and/or Requests for Quotations (or documents of similar effect) issued by City, and the responses thereto from the Contractor, and any document which purports to update or revise any of the foregoing; and (e) the results of any presentations or tests provided by the Contractor to the City. In the event of the conflict or inconsistency among the foregoing, the order of priority to resolve such conflict or inconsistency is as follows: firstly, any written amendments to this Agreement mutually agreed upon by the parties; secondly this Agreement; the items described in subsection (b) and (c); thirdly, the items described in subsection (d); and fourthly, the items described in subsection (e).

2.5 Marks

2.5.1 Marks shall mean the trademarks and/or trade names of Contractor as licensed to City hereunder.

2.6 Service Levels

2.6.1 The Contractor warrants that the Cloud Services will perform in accordance with the service levels as set out in Appendix 8 – Service Level Agreement.

2.6.2 The Contractor shall provide the City with incident reports regarding any unavailability of the Cloud Services that the Contractor becomes aware of.

2.7 Training

2.7.1. The Contractor shall provide a training plan in accordance with Appendix 1 – Scope of Services.

2.7.2 The City reserves the right to video and/or audio tape any and all training sessions, whether held at the City or the Contractor's site, or via teleconference. Use of such training

tapes shall be strictly for City staff training purposes and such training tapes may not be posted on any social media or otherwise made available to anyone other than City staff

2.8 WARRANTIES, REPRESENTATIONS AND COVENANTS

2.8.1 The City shall have the right to discontinue use of the Services for any reason and shall receive a full refund of all payments, for a period of ninety (90) calendar days after the Services Commencement Date (the “Warranty Period”).

2.8.2 Services Warranty. The Contractor represents and warrants that the Services provided to the City under this Agreement shall conform to, be performed, function, and produce results substantially in accordance with the Documentation. The Contractor shall offer the City warranty coverage equal to or greater than that offered by the Contractor to any of its customers.

2.8.3 The Contractor's obligations for breach of the Services Warranty shall be limited to using its best commercially reasonable efforts, at its own expense, to correct or replace that portion of the Services which fails to conform to such warranty, and, if the Contractor is unable to correct any breach in the Services Warranty by the date which is sixty (60) calendar days after the City provides notice of such breach, City may, in its sole discretion, either extend the time for the Contractor to cure the breach or terminate this Agreement and receive a full refund of all amounts paid to the Contractor under this Agreement.

2.8.4 Disabling Code Warranty. The Contractor represents, warrants and agrees that the Services do not contain and City will not receive from the Contractor any virus, worm, trap door, back door, timer, clock, counter or other limiting routine, instruction or design, or other malicious, illicit or similar unrequested code, including surveillance software or routines which may, or is designed to, permit access by any person, or on its own, to erase, or otherwise harm or modify any City system or Data (a "Disabling Code").

2.8.5 In the event a Disabling Code is identified, Contractor shall take all steps necessary, at no additional cost to City, to: (a) restore and/or reconstruct any and all Data lost by the City as a result of Disabling Code; (b) furnish to City a corrected version of the Services without the presence of Disabling Codes; and, (c) as needed, re-implement the Services at no additional cost to the City. This warranty shall remain in full force and effect as long as this Agreement remains in effect.

2.8.6 Intellectual Property Warranty. The Contractor represents, warrants and agrees that: Contractor has all Intellectual Property Rights necessary to provide the Services to the City in accordance with the terms of this Agreement; the Contractor is the sole owner or is a valid licensee of all software, text, pictures, audio, video, logos and copy that provides the foundation for provision of the Services, and has secured all necessary licenses, consents, and authorizations with respect to the use of these underlying elements; the Services do not and shall not infringe upon any patent, copyright, trademark or other proprietary right or violate any trade secret or other contractual right of any Third Party; and there is currently no actual or threatened suit against the Contractor by any Third Party based on an alleged violation of such right. This warranty shall survive the expiration or termination of this Agreement.

2.8.7 Warranty of Authority. Each party represents and warrants that it has the right to enter into this Agreement. The Contractor represents and warrants that it has the unrestricted

right to provide the Services, and that it has the financial viability to fulfill its obligations under this Agreement. The Contractor represents, warrants and agrees that the Services shall be free and clear of all liens, claims, encumbrances or demands of Third Parties. The Contractor represents and warrants that it has no knowledge of any pending or threatened litigation, dispute or controversy arising from or related to the Services. This warranty shall survive the expiration or termination of this Agreement.

2.8.8 Third Party Warranties and Indemnities. The Contractor will assign to the City all Third Party warranties and indemnities that the Contractor receives in connection with any products provided to the City. To the extent that the Contractor is not permitted to assign any warranties or indemnities through to the City, the Contractor agrees to specifically identify and enforce those warranties and indemnities on behalf of the City to the extent the Contractor is permitted to do so under the terms of the applicable third party agreements.

2.8.9 Date/Time Change Warranty. The Contractor represents and warrants to the City that the Services provided will accurately process date and time-based calculations under circumstances of change including, but not limited to: century changes and daylight saving time changes. The Contractor must repair any date/time change defects at the Contractor's own expense.

2.8.10 Most Favoured Customer Warranty. The Contractor represents and warrants and agrees that the Services and other fees stated herein are and shall be the lowest fees the Contractor charges any of its other customers. In any case where the City fees are found to be higher, then the Contractor will provide the City with a retroactive refund for any overpayment.

2.8.11 Resolution and Response Time Warranty: The Contractor warrants that all resolution and response times as delineated in Appendix 8 – Service Level Agreement shall be adhered to.

2.8.12 The warranties set forth above are in lieu of all other warranties, express or implied, with regard to the services pursuant to this Agreement, including, but not limited to, any implied warranties of merchantability and fitness for a particular purpose.

2.8.13 Errors and Omissions: Correction. The Contractor shall be responsible for the professional quality, technical accuracy, and the coordination of all designs, drawings, statement of work, and other services furnished by or on behalf of the Contractor under this Agreement. The Contractor, without additional compensation, shall correct or revise any errors or omissions in the designs, drawings, statement of work, and/or other Contractor services immediately upon notification by the City. The obligation provided for in this section with respect to any acts or omissions during the Term of this Agreement shall survive any termination or expiration of this Agreement and shall be in addition to all other obligations and liabilities of the Contractor.

2.9 Software Upgrades and Enhancements

2.9.1 The Contractor shall supply:

(a) at no additional cost updated versions of the Software to operate on upgraded versions of operating systems, upgraded versions of firmware, or upgraded versions of web browsers;

(b) at no additional cost interface softwares that are developed by the Contractor for interfacing the Cloud Services to other Software products; and

(c) at no additional cost, updated versions of the Cloud Services, that encompass improvements, extensions, maintenance updates, error corrections, or other changes that are logical improvements or extensions of the original Cloud Services supplied to the City.

2.9.2 Unless otherwise mutually agreed to in writing, the Contractor shall maintain any and all Third Party Software products at their most current version and at no additional charge. However, the Contractor shall not maintain any Third Party Software versions, including one version back, if any such version would prevent the City from using any functions, in whole or in part, or would cause deficiencies in the system. If implementation of an upgrade to a Third Party Software product requires personnel in addition to the staff proposed in the Response for the Hosted Services, the City and the Contractor shall discuss whether to implement such an upgrade and, if mutually agreed upon in writing, any additional charges to be paid by the City for such upgrade. Any additional costs that are charged by a Third Party Software manufacturer for an upgrade to a Third Party Software product that is not covered by such product's maintenance agreement shall be charged to and paid for by the Contractor.

2.9.3 Enhancements

The Contractor shall provide the City with all Enhancements and associated documentation that are provided as general releases to the Software, in whole or in part, as part of the Services. Such Documentation shall be adequate to inform the City of the problems resolved including any significant differences resulting from the release which are known by the Contractor. The Contractor warrants that each such Enhancement general release shall be tested and perform according to the requirements Specifications. The Contractor agrees to correct corrupted Data that may result from any system deficiency introduced by the Enhancement at no cost to the City. Enhancements to correct any Deficiency shall be provided to the City at no additional cost and without the need for a work order. Should the Contractor not be able to correct the hosted system so that it complies with the specifications in the Statement of Work and/or Service Level Agreement (SLA), to the City's reasonable satisfaction in a timely manner, the City may terminate this Agreement.

2.10 Performance Reporting

2.10.1 As part of the Services and at no additional cost to the City, the Contractor will, on a monthly basis during the Term, submit to the City a performance report (each, a "**Performance Report**"). Each Performance Report will describe in detail the effectiveness of the Services in meeting the City's requirements during the previous month, and in particular will address the following topics:

(a) the extent to which the City's minimum requirements for the Services as set out in this Agreement were met;

(b) if any minimum requirements were not met, a description of requirements that were not met and steps the Contractor took to remedy such failures;

(c) any other failures of the Services, including system unavailability, software errors, bugs, etc., including a description of the failure and steps the Contractor took to remedy such failure;

(d) any proposed improvements or upgrades to the Services to be implemented in the next following month; and
(e) such other performance measures as the City may reasonably request.

2.11 Optional Extension of Services

2.11.1 The City may, in its sole and absolute discretion, at any time after the first **X** months of the Term, upon written notice direct the Contractor to expand the Services to include such additional City departments, facilities or entities as the City may decide (a "**Services Expansion**"). The City may refer to the Performance Reports in considering a Services Expansion.

The following will apply with respect to any Services Expansion:

(a) the City and the Contractor will, acting reasonably, promptly enter into an amendment to this Agreement which will include any additional or amended terms as may be required to implement the Services Expansion; and
(b) the Contractor will be entitled to additional compensation for the performance of the additional services required for the Services Expansion, which will be determined on the basis of the Fees (as defined below).

2.11.2 For certainty, the City will not be obligated to issue any Services Expansion under this Agreement, and unless and until any Services Expansion is issued, the Contractor will only be entitled to perform the Services.

3. TIME

3.1 Time is of the essence.

4. TERM

4.1 The Contractor will provide the Services for a one (1) year period commencing on the Effective Date (the "Term").

4.2 The City may at any time prior to thirty (30) days before the end of the Term, by written notice to the Contractor, extend the Term for a period of time not to exceed three (3) one (1) year periods. If the City elects to extend the Term, the provisions of this Agreement will remain in force, including the Fees, except where amended in writing by the parties.

5. PERSONNEL

5.1 Personnel

5.1.1 The Contractor agrees at all times to maintain an adequate staff of experienced and qualified employees for efficient performance under this Agreement. The Contractor agrees that, at all times, the employees of the Contractor furnishing or performing any services shall do so in a proper, workmanlike, and dignified manner.

5.1.2 The Contractor agrees that all persons working for or on behalf of the Contractor whose duties bring them upon the City's premises shall obey the rules and regulations that are established by the City and shall comply with the reasonable directions of the City's

officers. The City may, at any time, require the removal and replacement of any of the Contractor's employees for good cause.

5.1.3 The Contractor shall be responsible for the acts of its employees and agents while on the Client's premises. Accordingly, the Contractor agrees to take all necessary measures to prevent injury and loss to persons or property located on the City's premises. The Contractor shall be responsible for all damages to persons or property caused by Vendor or any of its agents or employees. The Contractor shall promptly repair, to the specifications of the City, any damage that it, or its employees or agents, may cause to the City's premises or equipment; on the Contractor's failure to do so, the City may repair such damage and the Contractor shall reimburse the City promptly for the cost of repair.

5.1.4 The Contractor agrees that, in the event of an accident of any kind, the Contractor will immediately notify the City's contact person and thereafter, if requested, furnish a full written report of such accident.

5.1.5 The Contractor shall perform the services contemplated in the Agreement without interfering in any way with the activities of the City's staff or visitors.

5.1.6 The Contractor and its employees or agents shall have the right to use only those facilities of the City that are necessary to perform services under this Agreement and shall have no right to access any other facilities of the City. The City shall also extend parking privileges to properly identified members of the Contractor's full-time staff on the same basis as they are extended to City staff.

5.1.7 The City shall have no responsibility for the loss, theft, disappearance of, or damage to equipment, tools, materials, supplies, and other personal property of the Contractor or its employees, subcontractors, or material-men.

5.2 Sub-Contractors and Assignment

5.2.1 The Contractor will not engage any personnel or sub-contractors, or sub-contract or assign its obligations under this Agreement, in whole or in part, without the prior written approval of the City and any attempt to do so shall be void and without further effect.

5.2.2 Sub-contractor Disclosure: The Contractor shall identify all of its strategic business partners related to the Services provided under this Agreement, including but not limited to all sub-contractors or other entities or individuals who may be a party to a joint venture or similar agreement with the Contractor, and who shall be involved in any application development and/or operations.

5.3 Agreements with Sub-Contractors

5.3.1 The Contractor will preserve and protect the rights of the City with respect to any Services performed under sub-contract and incorporate the terms and conditions of this Agreement into all sub-contracts as necessary to preserve the rights of the City under this Agreement. The Contractor will be as fully responsible to the City for acts and omissions of sub-contractors and of persons directly or indirectly employed by them as for acts and omissions of persons directly employed by the Contractor.

5.4 Separation of Duties and Non-Disclosure

5.4.1 The Contractor shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of the City's data to that which is absolutely necessary to perform job duties.

5.5 Right to Remove Personnel

5.5.1 The City shall have the right at any time to require that the Contractor remove from interaction with the City any Contractor representative who the City believes is detrimental to its working relationship with the service provider. The City shall provide the Contractor with notice of its determination, and the reasons it requests the removal. If the public jurisdiction signifies that a potential security violation exists with respect to the request, the service provider shall immediately remove such individual. The Contractor shall not assign the person to any aspect of the contract or future work orders without the City's consent.

6. LIMITED AUTHORITY

6.1 Agent of City

6.1.1 The Contractor is not and this Agreement does not render the Contractor an agent or employee of the City, and without limiting the above, the Contractor does not have authority to enter into any contract or reach any agreement on behalf of the City, except for the limited purposes as may be expressly set out in this Agreement, or as necessary in order to provide the Goods and Services. The Contractor will make such lack of authority clear to all persons with whom the Contractor deals in the course of providing the Goods and Services.

6.2 Independent Contractor

6.2.1 The Contractor is an independent Contractor. This Agreement does not create the relationship of employer and employee, a partnership, or a joint venture. The City will not control or direct the details, means or process by which the Contractor performs the Services. The Contractor will determine the number of days and hours of work required to properly and completely perform the Services. The Contractor is primarily responsible for performance of the Services and may not delegate or assign any Services to any other person except as provided for in this Agreement. The Contractor will be solely liable for the wages, fringe benefits, work schedules and work conditions of any partners, employees or sub-contractors.

7. FEES AND PAYMENT

7.1 Fees

7.1.1 The City will pay to the Contractor the fees as set out in Appendix 2 – Fees and Payments (the "Fees"). Payment by the City of the Fees will be full payment for the Services and the Contractor will not be entitled to receive any additional payment from the City.

7.1.2 Fees for a particular Cloud Services server will begin to accrue when the Cloud Services server is associated with the City's account.

7.2 Payment – Subscription Fees

7.2.1 Subject to the provisions set out in Appendix 2 including the time of payments;

(a) The Contractor will submit an invoice (the **"Invoice")** to the City requesting payment of the Fees relating to the Cloud Services for the upcoming 12 months, and including the following information:

(1) an invoice number;
(2) the Contractor's name, address and telephone number;
(3) the City's reference number for the Services, PO # _____
(4) description and date of the Cloud Services;
(5) taxes (if any);
(6) other applicable charges (if any);
(7) Service Credits for non-compliance with the SLA (if applicable);
(8) grand total of the Invoice; and
(9) Contractor's representative Name, Title, Location and Department.

(b) if the City reasonably determines that any portion of an Invoice is not payable due to an error, then the City will so advise the Contractor;

(c) all Fees are payable in Canadian dollars; and

(d) no interest will be payable on any overdue accounts.

7.3 Payment Schedule – Subscription Fees

The City shall pay the Subscription Fee on an _____ basis, as described in Appendix 2 – Fees and Payments.

7.4 Payment – Professional Services

7.4.1 Subject to the provisions set out in Appendix 2 including the time of payments;

(a) The Contractor will submit an invoice (the **"Invoice")** to the City requesting payment of the Fees relating to the Professional Services provided in the previous month, and including the following information:

(1) an invoice number;
(2) the Contractor's name, address and telephone number;
(3) the City's reference number for the Services, PO # _____
(4) description and date(s) of professional services;
(5) Contractor's price per hour for each item, as per Appendix 2 – Fees and Payments, multiplied by the number of hours used of each item, and total for each item;
(6) taxes (if any);
(7) other applicable charges (if any);
(8) payment terms including any available prompt payment discounts;
(9) grand total of the Invoice; and
(10) Contractor's representative Name, Title, Location and Department.

(b) if the City reasonably determines that any portion of an Invoice is not payable due to an error, then the City will so advise the Contractor;

(c) all Fees are payable in Canadian dollars; and

(d) no interest will be payable on any overdue accounts.

7.5 Payment Schedule – Professional Services

The City shall pay the costs for any professional services on a time and material basis, as described in Appendix 2 – Fees and Payments in accordance with a statement of work to be mutually agreed upon by the parties for such professional services.

7.6 Invoicing

7.6.1 Invoices will be submitted by the Contractor by mail to: surreyinvoices@surrey.ca.

Name: City of Surrey – IT Project Management Office
Address: 13450 - 104th Avenue
Surrey, British Columbia V3T 1V8

Invoices and supporting documentation shall be prepared at the sole expense and responsibility of the Contractor. The City will not compensate the Contractor for any costs incurred for Invoice preparation. The City may request, in writing, changes to the content and format of the Invoice and supporting documentation at any time. The City reserves the right to request additional supporting documentation to substantiate costs at any time.

7.7 Records

7.7.1 The Contractor will prepare and maintain proper records related to the Services, including records, receipts and invoices relating to Disbursements. On request from the City, the Contractor will make the records available open to audit examination by the City at any time during regular business hours during the time the Contractor is providing the Services and for a period of six years after the Services are complete.

7.8 Non-Residents

7.8.1 If the Contractor is a non-resident of Canada and does not provide to the City a waiver of regulation letter, the City will withhold and remit to the appropriate governmental authority the greater of:

(a) 15% of each payment due to the Contractor; or
(b) the amount required under applicable tax legislation.

8. CITY RESPONSIBILITIES

8.1 City Information

8.1.1 The City will, in co-operation with the Contractor, make efforts to make available to the Contractor information which the City has in its files that relate to the delivery of the Services. The Contractor will review any such material upon which the Contractor intends to rely and take reasonable steps to determine if that information is complete or accurate. The Contractor will assume all risks that the information is complete and accurate and the Contractor will advise the City in writing if in the Contractor's judgment the information is deficient or unreliable and undertake such new surveys and investigations as are necessary.

8.2 City Decisions

8.2.1 The City will in a timely manner make all decisions required under this Agreement, examine documents submitted by the Contractor and respond to all requests for approval made by the Contractor pursuant to this Agreement.

8.3 Notice of Defect

8.3.1 If the City believes in good faith that some portion of the Services has not been completed satisfactorily, the City may require the Contractor to correct such work prior to the City making any payment. In such event, the City will provide the Contractor with an explanation of the concern and the remedy that the City expects. The City may withhold from any payment that is otherwise due, an amount that the City in good faith finds to be under dispute, of if the Contractor does not provide a sufficient remedy. The City may retain the amount equal to the cost to the City for otherwise correcting or remedying the work not properly completed.

9. INTELLECTUAL PROPERTY INFRINGEMENT INDEMNIFICATION

9.1 Contractor shall indemnify, defend and hold City harmless from any and all actions, proceedings, or claims of any type brought against City alleging that the Services and/or Documentation or City's use of the Services and/or Documentation constitutes a misappropriation or infringement upon any patent, copyright, trademark, or other proprietary right or violates any trade secret or other contractual right of any Third Party. Contractor agrees to defend against, and hold City harmless from, any claims and to pay all litigation costs, all reasonable attorneys' fees, settlement payments and all judgments, damages, costs or expenses awarded or resulting from any claim. City shall, after receiving notice of a claim, advise Contractor of it. City's failure to give Contractor timely notification of said claim shall not effect Contractor's indemnification obligation unless such failure materially prejudices Contractor's ability to defend the claim. City reserves the right to employ separate counsel and participate in the defense of any claim at its own expense.

9.2 If the Services and/or Documentation, or any part thereof, is the subject of any claim for infringement of any patent, copyright, trademark, or other proprietary right or violates any trade secret or other contractual right of any Third Party, or if it is adjudicated by a court of competent jurisdiction that the Services and/or Documentation, or any part thereof, infringes any patent, copyright, trademark, or other proprietary right or violates any trade secret or other contractual right of any Third Party, and City's use of the Services and/or Documentation, or any part of it, is enjoined or interfered with in any manner, Contractor shall, at its sole expense and within thirty (30) calendar days of such injunction or interference, either: (a) procure for City the right to continue using the Services and/or Documentation free of any liability for infringement or violation; (b) modify the Services and/or Documentation, or parts thereof, with non-infringing Services and/or Documentation of equivalent or better functionality that is reasonably satisfactory to City; or (c) replace the Services and/or Documentation, or parts thereof, with non-infringing Services and/or Documentation of equivalent or better functionality that is reasonably satisfactory to City.

9.3 Contractor shall have no obligation to indemnify City for a claim if: (a) City uses the Services in a manner contrary to the provisions of this Agreement and such misuse is the cause of the infringement or misappropriation; or (b) City's use of the Services in

combination with any product or system not authorized, approved or recommended by Contractor and such combination is the cause of the infringement or misappropriation.

9.4 No limitation of liability set forth elsewhere in this Agreement is applicable to the Intellectual Property Infringement Indemnification set forth herein.

10. INSURANCE AND DAMAGES

10.1 Indemnity

10.1.1 The Contractor will indemnify and save harmless the City and all of its elected and appointed officials, officers, employees, servants, representatives and agents (collectively the "**Indemnitees**"), from and against all claims, demands, causes of action, suits, losses, damages and costs, liabilities, expenses and judgments (including all actual legal costs) for damage to or destruction or loss of property, including loss of use, and injury to or death of any person or persons which any of the Indemnitees incur, suffer or are put to arising out of or in connection with any failure, breach or non-performance by the Contractor of any obligation of this Agreement, or any wrongful or negligent act or omission of the Contractor or any employee or agent of the Contractor.

10.1.2 City hereby agrees to indemnify and hold Contractor and its affiliates, sub-contractors and agents (and each of their respective shareholders, officers, directors, employees and Contractors) harmless from and against any and all third party claims and resulting losses and damages including, but not limited to, reasonable legal fees, fines and expenses, resulting from, relating to or arising out of (i) any breach of the terms and conditions of this Agreement by City or (ii) the negligence or willful misconduct of the City or its directors, officers, employees, contractors, or agents.

10.2 Survival of Indemnity

10.2.1 The indemnity described in sections 10.1.1 and 10.1.2 will survive the termination or completion of this Agreement and, notwithstanding such termination or completion, will continue in full force and effect for the benefit of the Indemnitees.

10.3 Limitation of Liability

10.3.1 In no event shall either party be liable for any loss of data, reprocurement costs, loss of profits, loss of use or for any other consequential, indirect, exemplary, special or incidental damages arising under or in connection with this Agreement, even if the other party has been advised of the possibility of such damages.

Neither party will be liable to the other for any indirect, incidental, special or consequential damages of any kind whatsoever and however caused, whether arising under contract, tort (including negligence) or otherwise, including (without limitation) loss of production, loss of or corruption to data, loss of profits or of contracts, loss of business, loss of management or operation time and lost of goodwill or anticipated savings, even if the party has been notified of the possibility thereof or could have foreseen such claims. The entire liability of each party to the other party for direct damages from any cause whatsoever, and regardless of the form of action or the cause of action, whether in contract or in tort (including negligence), strict liability, breach of a fundamental term, fundamental breach

or otherwise in connection with this Agreement. Liability will be limited to the limits of insurance coverage available.

10.4 Contractor's Insurance Policies

10.4.1 The Contractor will, without limiting its obligations or liabilities and at its own expense, provide and maintain throughout this Agreement the following insurances in forms and amounts acceptable to the City from insurers licensed to conduct business in Canada:

(a) commercial general liability insurance on an occurrence basis, in an amount not less than three million ($5,000,000) dollars inclusive per occurrence against death, bodily injury and property damage arising directly or indirectly out of the work or operations of the Contractor, its employees and agents. The insurance will include cross liability and severability of interests such that the coverage shall apply in the same manner and to the same extent as though a separate policy had been issued to each insured. The insurance will include, but not be limited to: premises and operators' liability, broad form products and completed operations, owners and Contractors protective liability, blanket contractual, employees as additional insureds, broad form property damage, non-owned automobile, contingent employers liability, personal injury, and incidental medical malpractice. The City will be added as additional insured; and

(b) professional errors and omissions insurance in an amount not less than one million ($2,000,000) dollars insuring all professionals providing the Services from liability resulting from errors or omissions in the performance of the Services, with a 12 month maintenance period.

10.5 Insurance Requirements

10.5.1 The Contractor will provide the City with evidence of the required insurance prior to the commencement of this Agreement. Such evidence will be in the form of a completed certificate of insurance acceptable to the City. The Contractor will, on request from the City, provide certified copies of all of the Contractor's insurance policies providing coverage relating to the Services, including without limitation any professional liability insurance policies. All required insurance will be endorsed to provide the City with thirty (30) days advance written notice of cancellation or material change restricting coverage. To the extent the City has an insurable interest, the builder's risk policy will have the City as first loss payee. The Contractor will be responsible for deductible amounts under the insurance policies. All of the Contractor's insurance policies will be primary and not require the sharing of any loss by the City or any insurer of the City.

10.6 Contractor's Responsibilities

10.6.1 The Contractor acknowledges that any requirements by the City as to the amount of coverage under any policy of insurance will not constitute a representation by the City that the amount required is adequate and the Contractor acknowledges and agrees that the Contractor is solely responsible for obtaining and maintaining policies of insurance in adequate amounts. The insurance policy coverage limits shall not be construed as relieving the Contractor from responsibility for any amounts which may exceed these limits, for which the Contractor may be legally liable.

10.7 Additional Insurance

10.7.1 The Contractor shall place and maintain, or cause any of its sub-contractor to place and maintain, such other insurance or amendments to the foregoing policies as the City may reasonably direct.

10.8 Waiver of Subrogation

10.8.1 The Contractor hereby waives all rights of recourse against the City for loss or damage to the Contractor's property.

11. TERMINATION

11.1 By the City

11.1.1 The City for any reason may with ninety (90) days written notice to the Contractor terminate this Agreement before the completion of the Term, such notice to be determined by the City at its sole discretion. Upon receipt of such notice, the Contractor will perform no further Services other than the work which is reasonably required to complete the Services. Despite any other provision of this Agreement, if the City terminates this Agreement before the completion of all the Services, the City will pay to the Contractor all amounts owing under this Agreement for Services provided by the Contractor up to and including the date of termination, plus reasonable termination costs in the amount as determined by the City in its sole discretion. Upon payment of such amounts no other or additional payment will be owed by the City to the Contractor, and, for certainty, no amount will be owing on account of lost profits relating to the portion of the Services not performed or other profit opportunities.

11.2 Termination for Cause

11.2.1 The City may terminate this Agreement for cause as follows:

(a) If the Contractor is adjudged bankrupt, or makes a general assignment for the benefit of creditors because of its insolvency, or if a receiver is appointed because of its insolvency, the City may, without prejudice to any other right or remedy the City may have, terminate this Agreement by giving the Contractor or receiver or trustee in bankruptcy written notice; or

(b) If the Contractor is in breach of any term or condition of this Agreement, and such breach is not remedied to the reasonable satisfaction of the City within 5 days after delivery of written notice from the City to the Contractor, then the City may, without prejudice to any other right or remedy the City may have, terminate this Agreement by giving the Contractor further written notice.

11.2.2 If the City terminates this Agreement as provided by this Section, then the City may:

(a) enter into contracts, as it in its sole discretion sees fit, with other persons to complete the Services;

(b) withhold payment of any amount owing to the Contractor under this Agreement for the performance of the Services;

(c) set-off the total cost of completing the Services incurred by the City against any amounts owing to the Contractor under this Agreement, and at the completion of the Services pay to the Contractor any balance remaining; and

(d) if the total cost to complete the Services exceeds the amount owing to the Contractor, charge the Contractor the balance, which amount the Contractor will forthwith pay.

11.3 Curing Defaults

11.3.1 If either party is in default of any of its obligations under this Agreement, then either party may without terminating this Agreement, upon fourteen (14) days written notice to the defaulting party, remedy the default and set-off all costs and expenses of such remedy against any amounts owing to the defaulting party. Nothing in this Agreement will be interpreted or construed to mean that the non-defaulting party has any duty or obligation to remedy any default of the defaulting party. Parties agree to act reasonably and diligently to remedy issues.

12. APPLICABLE LAWS

12.1 Applicable Laws

12.1.1 This Agreement will be governed by and construed in accordance with the laws of the Province of British Columbia. The City and the Contractor accept the jurisdiction of the courts of British Columbia and agree that any action under this Agreement be brought in such courts.

12.2 Codes and By-Laws

12.2.1 The Contractor will provide the Services in full compliance with all applicable laws and regulations.

12.3 Interpretation of Laws

12.3.1 The Contractor will, as a qualified and experienced professional, interpret laws and regulations applicable to the performance of the Services. If an authority having jurisdiction imposes an interpretation which the Contractor could not reasonably have verified or foreseen prior to entering into this Agreement, then the City will pay the additional costs, if any, of making alterations so as to conform to the required interpretation.

13. DATA PRIVACY

13.1 The Contractor will use City Data only for the purpose of fulfilling its duties under this Agreement and for City's sole benefit, and will not share such Data with or disclose it to any Third Party without the prior written consent of City or as otherwise required by law. By way of illustration and not of limitation, Contractor will not use such Data for Contractor's own benefit and, in particular, will not engage in "data mining" of City Data or communications, whether through automated or human means, except as specifically and expressly required by law or authorized in writing by City.

13.2 All City Data will be stored on servers located solely within Canada.

13.3 The Contractor will provide access to City Data only to those Contractor employees, contractors and subcontractors who need to access the Data to fulfill Contractor obligations under this Agreement. The Contractor will ensure that, prior to being granted access to the Data, Contractor staff who perform work under this Agreement have all undergone and passed criminal background screenings; have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all Data protection provisions of this Agreement; and possess all qualifications appropriate to the nature of the employees' duties and the sensitivity of the Data they will be handling.

13.4 The Contractor will ensure it maintains the confidentiality, integrity and availability of City Data by ensuring appropriate security controls are applied as set forth in Section 15.1.

14. CONFIDENTIALITY AND DISCLOSURE OF INFORMATION

14.1 No Disclosure

14.1.1 Except as provided for by law or otherwise by this Agreement, the Contractor and the City will keep strictly confidential any information supplied to, obtained by, or which comes to the knowledge of the Contractor and the City as a result of the performance of the Services and this Agreement, and will not, without the prior express written consent of the Contractor and the City, publish, release, disclose or permit to be disclosed any such information, (the "Confidential Information") to any person or corporation, either before, during or after termination of this Agreement, except as reasonably required to complete the Services.

14.2 Freedom of Information and Protection of Privacy Act

14.2.1 The Contractor acknowledges that the City is subject to the *Freedom of Information and Protection of Privacy Act* of British Columbia and agrees to any disclosure of information by the City required by law.

Refer to Schedule 1 Privacy Protection Schedule, and Refer to Schedule 2 Confidentiality Agreement.

14.2.2 The Privacy Protection Schedule and Confidentiality Agreement attached to this Agreement form a part of and is incorporated into this Agreement.

14.3 Return of Property and City Data

14.3.1 The Contractor agrees to return to the City all of the City's property including any and all Data at the completion of this Agreement, upon the City's written request made within thirty (30) days after such termination or expiration, as provided herein. This provision applies to all City Data that is in the possession of subcontractors, agents or auditors of Contractor. Within fifteen (15) days after the date of the City's request , the Contractor will make available to City for download a file of City Data in an agreed-upon machine readable (a commercially-reasonable standard such as comma separated value (.csv) or extendible markup language (.xml)) format along with attachments in their native format as stored on the Cloud Services. Such service shall be done at no cost to the City. Once contractor has received written confirmation from City that all City Data has been

successfully transferred to the City, Contractor shall within thirty (30) days, unless legally prohibited, purge or physically destroy all City Data from its hosted servers or files and provide City with written certification in accordance with Section 15.6 herein.

15. SECURITY

15.1 Security

The Contractor shall disclose its non-proprietary security processes and technical limitations to the City such that adequate protection and flexibility can be attained between the City and the Contractor. For example: virus checking and port sniffing – the City and the Contractor shall understand each other's roles and responsibilities. The Contractor and the City recognize that security responsibilities are shared. The Contractor is responsible for providing a secure application services and/or infrastructure within the context of the services being provided to the City. The City is responsible for securing City owned and operated infrastructure.

15.2 Access to Data, Security Logs and Reports

The Contractor shall provide reports to the City in a format as specified in the service level agreement (SLA) agreed to by both the Contractor and the City. Reports shall include latency statistics, user access, user access IP address, user access history and security logs for all City files related to this Agreement. Audit logs and login history logs shall include the following requirements:

(1) Audit logs (in a filterable and exportable.csv format): user, date and time of change (add or update), previous value of field, current value of the field, object; and

(2) Login history logs: IP address that attempted login, date and time and success/fail.

15.3 Import and Export of Data

The City shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Contractor. This includes the ability for the City to import or export data to/from other service providers.

15.4 Access To and Extraction of City Data

The City shall have access to City's Data during the Term. Contractor shall within seven (7) business days of City's request, provide City, without any contingencies whatsoever (including but not limited to payment of any fees due to contractor), an extract of the data in a mutually agreed upon machine readable format, anytime during the term of this Agreement. Such provision of City Data, shall be charged to the City on a time and materials basis, as agreed to by the parties, at the hourly rates of the Contractor as set out in Appendix 5 – Professional Services.

15.5 Data Ownership

All Data shall become and remain the property of the City.

15.6 Data Protection

Protection of personal privacy and Data shall be an integral part of the business activities of the service provider to ensure there is no inappropriate or unauthorized use of City information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of Data and comply with the following conditions:

(a) The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Information and Data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own Personal Information and Data of similar kind;

(b) Without limiting the foregoing, the Contractor warrants that all City Data will be encrypted in transmission (including via web interface) using Transport Layer Security (TLS) at an encryption level equivalent to or stronger than 128-bit AES encryption. Further, the Contractor warrants that all City Data will be encrypted while in storage at an encryption level equivalent to or stronger than 256-bit AES encryption;

(c) At no time shall any Data or processes — that either belong to or are intended for the use of the City or its officers, agents or employees — be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the City;

(d) The Contractor shall not use any information collected in connection with the service issued from this Agreement for any purpose other than fulfilling the service;

(e) All facilities used to store and process City Data will implement and maintain administrative, physical, technical, and procedural safeguards and best practices at a level sufficient to secure such City Data from unauthorized access, destruction, use, modification, or disclosure. Such measures will be no less protective than those used to secure Contractor's own data of a similar type, and in no event less than reasonable in view of the type and nature of the Data involved; and

(f) The Contractor shall at all times use industry-standard and up-to-date security controls, technologies and procedures including, but not limited to firewalls, strong authentication, anti-malware protections, intrusion detection and prevention, regular patch management and vulnerability scanning, security event logging and reporting, and transport and storage encryption in providing the Services under this Agreement.

15.6.1 Prior to the "Go Live" Date the Contractor will at its expense conduct or have conducted the requirements in subsections (a), (b) and (c) and thereafter, the Contractor will at its expense conduct or have conducted the requirements in subsections (a), (b) and (c) at least once per year, and immediately after any actual or reasonably suspected Data Breach:

(a) Audit of Contractor's security policies, procedures and controls;

(b) A vulnerability scan, performed by a City-approved Third Party, of Contractor's systems and facilities that are used in any way to deliver Services under this Agreement; and

(c) A formal penetration test, performed by a process and qualified personnel of Contractor's systems and facilities that are used in any way to deliver Services under this Agreement.

Any time during the Term, if the Contractor intends to use data facilities of a different hosting service provider for storing the City Data, the Contractor shall provide at least thirty (30) days prior written notice of its intention to the City with proof in writing of the new hosting service provider meeting the requirements of being certified under ISO 27017 (or standards that succeed them, and which are acknowledged by both parties as equally or more effective). For greater clarity, failing to do so, would result in a substantial breach of the contract as per Section 11.2.2.

15.6.2 The Contractor will provide City the reports or other documentation resulting from the above audits, certifications, scans and tests in 15.5.1(a), 15.5.1(b) and 15.5.1(c) within seven (7) business days of the Contractor's receipt of a request from the City.

15.6.3 Based on the results of the above audits, certifications, scans and tests, the Contractor will, within thirty (30) calendar days of receipt of such results, promptly modify its security measures in order to meet its obligations under this Agreement, and provide the City with written evidence of remediation, Based on the results of the above audits, certifications, scans and tests, the Contractor will, within thirty (30) calendar days of receipt of such results, promptly modify its security measures in order to meet its obligations under this Agreement, and provide the City with written evidence of remediation, provided that to the extent that completing such modifications to its security measures is not practicable within thirty (30) calendar days, the Contractor will have commenced such modifications within thirty (30) calendar days and will thereafter diligently pursue the implementation until completion within one hundred and eighty (180) days.

15.6.4 The City may require, at its expense, that the Contractor perform additional audits and tests, and the Contractor will use commercially reasonable efforts, taking into consideration the availability of its resources, to accommodate such request. Any audit or test request by the City needs to be coordinated with the Contractor and will be performed only on a mutually agreed basis including the timeline for the audit or test. When performed, the results of any such audit or test will be provided to the City within seven (7) business days of the Contractor's receipt of such results. The City shall reimburse the Contractor for all its reasonable out of pocket expenses in connection with such audit or test, including the cost of the Contractor staff used for such audit.

15.7 Data Destruction

15.7.1 The Contractor acknowledges and agrees that, upon termination or expiry of this Agreement, or at any time during the term of this Agreement at the City's request, all City data in the possession of the Contractor shall be destroyed using a "Purge" or "Destroy" method, as defined by NIST Special Publication 800-88, such that ensures that data recovery is infeasible.

15.7.2 The Contractor must provide the City with a backup of all Data prior to performing data destruction unless otherwise instructed by the City in writing. The Contractor must receive confirmation from the City that all Data to be destroyed has been received.

15.7.3 The Contractor agrees to provide a "Certificate of Sanitization/Disposition" within a reasonable period of performing Data Destruction for each piece of media that has been sanitized which includes, at a minimum, the following information:

- Type of Media Sanitized;

- Description of Sanitization Process and Method Used;
- Tool Used for Sanitization;
- Verification Method;
- Date of Sanitization; and
- Signature of Contractor.

16. SECURITY INCIDENT OR DATA BREACH RESPONSE

16.1 When either a Security Incident or a Data Breach is suspected, investigation is required to commence without delay. If the Contractor becomes aware of a suspected Security Incident or suspected Data Breach, the Contractor will inform the City Clerk immediately (unless a Data Breach is conclusively ruled out, in which case notification must be within 24 hours) by contacting the City's 24x7 IT on-call staff at 604-591-4444 and selecting the option for critical services.

16.2 If a Data Breach is confirmed, immediate remedial action is required; the Contractor must notify the City Clerk immediately by contacting the City's 24x7 IT on-call staff as described above.

16.3 Immediately upon becoming aware of any suspected Security Incident, the Contractor shall fully investigate the Security's Incident's circumstances, extent and causes. The Contractor must then report the results to City Clerk and continue to keep City Clerk informed on a daily basis of the progress of its investigation until the issue has been effectively resolved.

16.4 Oral reports by the Contractor regarding Security Incidents and Data Breaches will be reduced to writing and supplied to the City Clerk as soon as reasonably practicable, but in no event more than forty-eight (48) hours after the oral report.

16.5 For any confirmed Security Incident, the Contractor's report discussed herein shall identify: (i) the nature of the incident, (ii) the cause or suspected cause of the incident, (iii) what the Contractor has done or shall do to mitigate the incident. and (iv) what corrective action Contractor has taken or shall take to prevent future similar incidents.

16.6 For an actual or suspected Data Breach, the Contractor's report discussed herein shall identify: (i) the nature of the unauthorized use or disclosure, (ii) the Data used or disclosed, (iii) who made the unauthorized use or received the unauthorized disclosure (if known), (iv) what Contractor has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and (v) what corrective action Contractor has taken or shall take to prevent future similar unauthorized use or disclosure.

16.7 Contractor, at its expense, shall cooperate fully with City's investigation of and response to any Data Breach, including allowing the City to participate as is legally permissible in the breach investigation.

16.8 Contractor will not provide notice of the Data Breach directly to the persons whose Data were involved, regulatory agencies, or other entities, without prior written permission from City.

16.9 Notwithstanding any other provision of this Agreement, and in addition to any other remedies available to City under law or equity, Contractor will promptly reimburse City in full for all costs incurred by City in any investigation, remediation or litigation resulting from any Data Breach, including but not limited to providing notification to Third Parties whose Data were compromised and to regulatory bodies, law enforcement agencies or other entities as required by law or contract; establishing and monitoring call center(s), and credit monitoring and/or identity restoration services to assist each person impacted by a Data Breach in such a fashion that, in City's sole discretion, could lead to identity theft; and the payment of legal fees and expenses, audit costs, fines and penalties, and other fees imposed by regulatory agencies, courts of law, or contracting partners as a result of the Data Breach.

17. INTELLECTUAL PROPERTY RIGHTS

17.1 Intellectual Property is owned by the applicable content owner and, except as expressly set out herein, this Agreement does not grant either party any rights, implied or otherwise, to the other's Intellectual Property. For greater certainty:

(a) The City acknowledges that the Contractor retains all right, title and interest in the Intellectual Property. The City acknowledges that it does not, by virtue of receiving a license to use the Intellectual Property, acquire any proprietary rights therein, other than the limited rights granted in this Agreement. The Contractor warrants that it is the sole owner of the Intellectual Property; and

(b) The Contractor acknowledges that the City retains all right, title and interest in the City's Intellectual Property. The Contractor acknowledges that it does not, by virtue of receiving a license to use the City's Intellectual Property in order to customize the Intellectual Property, acquire any proprietary right to the City's Intellectual Property, other than the limited rights granted under this Agreement. The City warrants that it owns the Intellectual Property that it provides to the Contractor for the purpose of customizing the Intellectual Property.

17.2 Neither party may transfer or assign its rights and obligations under this Agreement without first obtaining the other party's prior written consent.

17.3 Upon termination or expiry of this Agreement the Contractor shall remove the City's Intellectual Property from the software.

18. PROTECTION OF PERSONAL INFORMATION

18.1 Refer to Appendix 6 – Privacy Protection Schedule.

19. RESPONSE TO LEGAL ORDERS, DEMANDS OR REQUESTS FOR DATA

19.1 Except as otherwise expressly prohibited by law, the Contractor will:

(a) If required by a court of competent jurisdiction or an administrative body to disclose City Data, Contractor will notify City in writing immediately upon receiving notice of such requirement and prior to any such disclosure;

(b) Consult with City regarding its response;

(c) Cooperate with City's reasonable requests in connection with efforts by City to intervene and quash or modify the legal order, demand or request; and

(d) Upon City's request, provide City with a copy of its response.

19.2 If City receives a subpoena, warrant, or other legal order, demand or request seeking City Data maintained by Contractor, City will promptly provide a copy to Contractor. Contractor will supply City with copies of Data required for City to respond within forty-eight (48) hours after receipt of copy from City, and will cooperate with City's reasonable requests in connection with its response.

20. DATA RETENTION AND DISPOSAL

20.1 City Records fall under the City's retention policies, not the Contractors. The Corporate Records program is governed by the *Corporate Records By-law, 2010, No. 17002*, adopted by Council on March 22, 2010.

21. DATA TRANSFER UPON TERMINATION OR EXPIRATION

21.1 Upon termination or expiration of this Agreement, Contractor, or a new owner (s) in the event of a merger, takeover or new partnership, will ensure that all City Data are securely transferred to City, or a Third Party designated by City, within ten (10) calendar days of any such event, all as further specified in the technical specifications attached as APPENDIX 1-A. Contractor will ensure that such migration uses facilities and methods that are compatible with the relevant systems of City, and that City will have access to City Data during the transition. In the event that it is not possible to transfer the aforementioned Data to City in a format that does not require proprietary software to access the Data, Contractor shall provide City with an unlimited use, perpetual license to any proprietary software necessary in order to gain access to the Data.

21.2 Contractor will provide a fully documented service description and perform and document a gap analysis by examining any differences between its Services and those to be provided by its successor.

21.3 Contractor will provide a full inventory and configuration of servers, routers, other hardware, and software involved in service delivery along with supporting documentation, indicating which if any of these are owned by or dedicated to City.

21.4 Contractor shall implement its contingency and/or exit plans and take all necessary actions to provide for an effective and efficient transition of service with minimal disruption to City. Contractor will work closely with its successor to ensure a successful transition to the new service and/or equipment, with minimal downtime and effect on City, all such work to be coordinated and performed no less than ninety (90) calendar days in advance of the formal, final transition date.

22. INTERRUPTIONS IN SERVICE; SUSPENSION AND TERMINATION OF SERVICE; CHANGES TO SERVICE

22.1 The City may suspend or terminate (or direct the Contractor to suspend or terminate) an end user's access to Services in accordance with the City's policies. The City will assume sole responsibility for any claims made by end user regarding the City's suspension/termination or directive to suspend/terminate such Services.

22.2 The Contractor may suspend access to Services by the City immediately in response to an act or omission that reasonably appears to jeopardize the security or integrity of Contractor's Services or the network(s) or facilities used to provide the Services.

Suspension will be to the minimum extent, and of the minimum duration, required to prevent or end the security issue. The suspension will be lifted immediately once the breach is cured. The Contractor may suspend access to Services by the City in response to a material breach by the City of any terms of use the City has agreed to in connection with receiving the Services. The Contractor will immediately notify the City of any suspension of the City access to Services.

23. RIGHTS AND LICENSE IN AND TO CITY DATA

23.1 The parties agree that as between them, all rights, in and to City Data shall remain the exclusive property of the City, and the Contractor has a limited, nonexclusive license to access and use these Data as provided in this Agreement solely for the purpose of performing its obligations hereunder.

23.2 All City Data created and/or processed by the Services is and shall remain the property of the City and shall in no way become attached to the Services, nor shall Contractor have any rights in or to the Data of the City.

23.3 This Agreement does not give a party any rights, implied or otherwise, to the other's Data, content, or intellectual property, except as expressly stated in the Agreement.

23.4 The City retains the right to use the Services to access and retrieve City Data stored on Contractor's Services infrastructure at any time at its sole discretion.

23.5 The Contractor shall agree to support the City to conduct a Data export annually for archiving purposes.

24. ESCROWING OF SOURCE CODE OF LICENSED SOFTWARE

24.1 After the parties execution of this Agreement and at written request of City, the parties shall enter into a Source Code Escrow Agreement with a mutually agreed third-party escrow agent ("**Escrow Agent**") pursuant to which the Contractor will deposit a source code version of the software component of the Cloud Services other than any third party software with all necessary passwords, software keys, and related technical documentation (collectively, the "Source Code").

24.2 Each of the following shall constitute a "**Release Event**" for purposes of this Agreement and the Source Code Escrow Agreement:

(a) In the event that the Contractor:

(i) makes an assignment in bankruptcy, or is subject to a bankruptcy order, under the Bankruptcy and Insolvency Act (Canada) or the bankruptcy and insolvency legislation of any other jurisdiction;

(ii) has made a general assignment for the benefit of its creditors; or

(iii) has terminated its on-going business operations or transfers all or substantially all of the assets or obligations associated with or set forth in this Agreement to a third party except in connection with a continuation of the Contractor's business;

provided that, if the Contractor (A) is still providing the Cloud Services to the City; and (B) is disputing an involuntary assignment or order described in subsection (i) or (ii) above,

the Contractor shall have forty (40) calendar days after the receipt of the assignment or order, failing which a "Release Event" is deemed to have occurred.

24.3 All rights and licenses granted by Contractor under this Agreement or the Source Code Escrow Agreement (including all licensed Software, Source Code, documentation and work product, are and shall be deemed to be rights and licenses to "intellectual property, "as such term is used in and interpreted under Section 65.11(7) of the Bankruptcy and Insolvency Act (Canada) and Section 32(6) of the Companies' Creditors Arrangement Act (Canada) and the Escrow Agreement is "supplementary" to this Agreement. In each case, the City shall have all rights, elections and protections under the Bankruptcy and Insolvency Act (Canada), the Companies Creditors Arrangement Act (Canada) and all other applicable bankruptcy, insolvency, restructuring and similar laws with respect to this Agreement, the Source Code Escrow Agreement and the subject matter hereof and thereof.

24.4 Escrow Fees. All fees and expenses charged by an escrow agent will be borne by the City.

25. WORKERS' COMPENSATION BOARD, AND OCCUPATIONAL HEALTH AND SAFETY

25.1 The Contractor will, at its own expense, procure and carry full Workers' Compensation Board coverage for itself and all workers, employees, servants and others engaged in the supply of the Goods and Services. The City has the unfettered right to set off the amount of the unpaid premiums and assessments for the Workers' Compensation Board coverage against any monies owning by the City to the Contractor. The City will have the right to withhold payment under this Agreement until the Workers' Compensation Board premiums, assessments or penalties in respect of the Goods and Services have been paid in full.

25.2 The Contractor will provide the City with the Contractor's Workers' Compensation Board registration number and a letter from the Worker's Compensation Board confirming that the Contractor is registered in good standing with the Workers' Compensation Board.

25.3 The Contractor agrees that it is the prime contractor for the Services for the purposes of the *Workers Compensation Act*, unless the City specifies in writing that it is not. The Contractor will have a safety program in place that meets the requirements of the Workers' Compensation Board Occupational Health and Safety Regulation and the *Workers Compensation Act*. As prime contractor, the Contractor will be responsible for appointing a qualified coordinator for insuring the health and safety activities for the location of the Services. That person will be the person so identified in this Agreement, and the Contractor will advise the City immediately in writing if the name or contact number of the qualified coordinator changes.

25.4 Without limiting the generality of any other indemnities granted by the Contractor in this Agreement, the Contractor will indemnify and save harmless the Indemnitees from and against all claims, demands, causes of action, suits, losses, damages, costs, liabilities,

expenses, judgments, penalties and proceedings (including all actual legal costs) which any of the Indemnitees incur, suffer or are put to arising out of or in any way related to unpaid Workers' Compensation Board assessments owing from any person or corporation engaged in the performance of this Agreement or arising out of or in any way related to the failure to observe safety rules, regulations and practices of the Workers' Compensation Board, including penalties levied by the Workers' Compensation Board.

25.5 The Contractor will ensure compliance with and conform to all health and safety laws, by-laws or regulations of the Province of British Columbia, including without limitation the *Workers Compensation Act* and Regulations pursuant thereto.

25.6 The City may, on twenty-four (24) hours written notice to the Contractor, install devices or rectify any conditions creating an immediate hazard existing that would be likely to result in injury to any person. However, in no case will the City be responsible for ascertaining or discovering, through inspections or review of the operations of the Contractor or otherwise, any deficiency or immediate hazard.

26. DISPUTE RESOLUTION

26.1 Dispute Resolution Procedures

The parties will make reasonable efforts to resolve any dispute, claim, or controversy arising out of this Agreement or related to this Agreement ("**Dispute**") using the dispute resolution procedures set out in this section 26.

(a) Negotiation

The parties will make reasonable efforts to resolve any Dispute by amicable negotiations and will provide frank, candid and timely disclosure of all relevant facts, information and documents to facilitate negotiations.

(b) Mediation

If all or any portion of a Dispute cannot be resolved by good faith negotiations within 30 days, either party may by notice to the other party refer the matter to mediation. Within 7 days of delivery of the notice, the parties will mutually appoint a mediator. If the parties fail to agree on the appointment of the mediator, then either party may apply to the British Columbia International Commercial Arbitration Centre for appointment of a mediator. The parties will continue to negotiate in good faith to resolve the Dispute with the assistance of the mediator. The place of mediation will be Surrey, British Columbia. Each party will equally bear the costs of the mediator and other out-of-pocket costs, and each party will bear its own costs of participating in the mediation.

(c) Litigation

If within 90 days of the request for mediation the Dispute is not settled, or if the mediator advises that there is no reasonable possibility of the parties reaching a negotiated resolution, then either party may without further notice commence litigation.

27. JURISDICTION AND COUNCIL NON-APPROPRIATION

27.1 Nothing in this Agreement limits or abrogates, or will be deemed to limit or abrogate, the jurisdiction of the Council of the City in the exercise of its powers, rights or obligations under any public or private statute, regulation or by-law or other enactment.

27.2 The Contractor recognizes and agrees that the City cannot make financial commitments beyond the City's current fiscal year. The City will annually make bonafide requests for appropriation of sufficient funds to cover all payments covered by this Agreement. If City Council does not appropriate funds, or appropriates insufficient funds, the City will notify the Contractor of its intention to terminate or reduce the services so affected within 90 days after the non-appropriation becomes final. Such termination shall take effect 90 days from the date of notification, shall not constitute an event of default and shall relieve the City, its officers and employees, from any responsibility or liability for the payment of any further amounts under this Agreement.

28. GENERAL

28.1 Entire Agreement

This Agreement, including the Appendices and any other documents expressly referred to in this Agreement as being a part of this Agreement, contains the entire agreement of the parties regarding the provision of the Services and no understandings or agreements, oral or otherwise, exist between the parties except as expressly set out in this Agreement. This Agreement supersedes and cancels all previous agreements between the parties relating to the provision of the Services.

28.2 Amendment

This Agreement may be amended only by agreement in writing, signed by both parties.

28.3 Contractor’s Terms Rejected

In the event that the Contractor issues an invoice, packing slip, sales receipt, or any like document to the City, the City accepts the document on the express condition that any terms and conditions in it which constitute terms and conditions which are in addition to or which establish conflicting terms and conditions to those set out in this Agreement are expressly rejected by the City.

28.4 Survival of Obligations

All of the Contractor's obligations to perform the Services in a professional and proper manner will survive the termination or completion of this Agreement.

28.5 Cumulative Remedies

The City’s remedies under this Agreement are cumulative and in addition to any right or remedy which may be available to the City at law or in equity.

28.6 Notices

Any notice, report or other document that either party may be required or may wish to give to the other must be in writing, unless otherwise provided for, and will be deemed to be validly given to and received by the addressee, if delivered personally, on the date of such personal delivery, if delivered by facsimile, on transmission, or if by mail or email, five calendar days after posting. The addresses for delivery will be as follows:

(a) The City:

City of Surrey – IT Department
13450 - 104th Avenue
Surrey, British Columbia, Canada, V3T 1V8

Attention:
Fax:
E-mail:

(b) The Contractor:

[Company Name]
[Street Address], [City], [Province/State] [Postal or Zip Code]

Attention: [Contact Name/Position Title]
Fax:
E-mail:

28.7 Unenforceability

If any provision of this Agreement is invalid or unenforceable, it will be severed from the Agreement and will not affect the enforceability or validity of the remaining provisions of the Agreement.

28.8 Headings

The headings in this Agreement are inserted for convenience of reference only and will not form part of nor affect the interpretation of this Agreement.

28.9 Singular, Plural and Gender

Wherever the singular, plural, masculine, feminine or neuter is used throughout this Agreement the same will be construed as meaning the singular, plural, masculine, feminine, neuter or body corporate where the context so requires.

28.10 Waiver

No waiver by either party of any breach by the other party of any of its covenants, obligations and agreements will be a waiver of any subsequent breach or of any other covenant, obligation or agreement, nor will any forbearance to seek a remedy for any breach be a waiver of any rights and remedies with respect to such or any subsequent breach.

28.11 Signature

This Agreement may be executed in or one or more counterparts all of which when taken together will constitute one and the same agreement, and one or more of the counterparts may be delivered by fax or PDF email transmission.

28.12 Force Majeure

Neither party shall be liable to the other for failure or delay of performance hereunder due to causes beyond its reasonable control. Such delays include, but are not limited to, earthquake, flood, storm, fire, epidemics, acts of government, governmental agencies or officers, war, riots, or civil disturbances. The non-performing party will promptly notify the other party in writing of an event of force majeure, the expected duration of the event, and its anticipated effect on the ability of the party to perform its obligations, and make reasonable effort to remedy the event of force majeure in a timely fashion.

The performing party may terminate or suspend its performance under this Agreement if the non-performing party fails to perform its obligations under this Agreement for more than fifteen (15) consecutive calendar days. City's payment obligations shall be suspended automatically if it is denied access to the Services for more than five (5) hours in any twenty-four (24) hour period.

[Signature page follows]

28.13 Enurement

This Agreement shall enure to the benefit of and be binding upon the respective successors and permitted assigns of the City and the Contractor.

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

CITY OF SURREY
by its authorized signatory:

_____
(Signature of Authorized Signatory)

_____
(Print Name and Position of Authorized Signatory)

<<INSERT NAME OF CONTRACTOR>>
I/We have the authority to bind the Contractor.

_____
(Legal Name of Contractor)

_____	_____
(Signature of Authorized Signatory)	(Signature of Authorized Signatory)
_____	_____
(Print Name and Position of Authorized Signatory)	(Print Name and Position of Authorized Signatory)

(APPENDICES 1 THROUGH 8 WILL BE INSERTED LATER WHEN AN AGREEMENT IS ASSEMBLED FOR EXECUTION INCLUDING INFORMATION FROM THE RFQ AND SUCCESSFUL PROPOSAL.)

APPENDIX 1 – SCOPE OF SERVICES

APPENDIX 1-A – FUNCTIONAL AND TECHNICAL REQUIREMENTS

APPENDIX 2 – FEES AND PAYMENT

APPENDIX 3 – TIME SCHEDULE

APPENDIX 4 – KEY PERSONNEL AND SUB-CONSULTANTS

APPENDIX 5 – PROFESSIONAL SERVICES

APPENDIX 6 – PRIVACY PROTECTION SCHEDULE

APPENDIX 7 – CONFIDENTIALITY AGREEMENT

APPENDIX 8 – SERVICE LEVEL AGREEMENT

SCHEDULE C – QUOTATION

RFQ Project Title: **Emergency Notification System**

RFQ Reference No.: **1220-040-2019-095**

Legal Name of Contractor: _____

Contact Person and Title: _____

Business Address: _____

Telephone: _____

Fax: _____

E-Mail Address: _____

TO:

City Representative: Richard D. Oppelt, Manager, Procurement Services

Address: Surrey City Hall
Finance & Technology Department – Purchasing Section
Reception Counter, 5th Floor West
13450 – 104 Avenue, Surrey, B.C., Canada V3T 1V8

E-mail for PDF Files: purchasing@surrey.ca.

1.0 If this Quotation is accepted by the City, a contract will be created as described in the RFQ.

2.0 **I/We confirm** that the following schedules are attached to and form a part of this Quotation:

Schedule C-1 – Statement of Departures;
Schedule C-2 – Contractor's Experience, Reputation and Resources;
Schedule C-3 – Contractor's Technical Quotation (Services);
Schedule C-3-1 – Function and Technical Requirements
Schedule C-4 – Contractor's Technical Quotation (Time Schedule); and
Schedule C-5 – Contractor's Financial Quotation:
Schedule C-5-1 – Financial Worksheet.

3.0 **I/We confirm** that this Quotation is accurate and true to best of my/our knowledge.

4.0 **I/We confirm** that, if I/we am/are awarded a contract, I/we will at all times be the "prime contractor" as provided by the *Worker's Compensation Act (British Columbia)* with respect to the Services. I/we further confirm that if I/we become aware that another contractor at the place(s) of the Services has been designated as the "prime contractor", I/we will notify the City immediately, and I/we will indemnify and hold the City harmless against any claims, demands, losses, damages, costs, liabilities or expenses suffered by the City in connection with any failure to so notify the City.

This Quotation is submitted this ____day of _____, 2016**.**

I/We have the authority to bind the Contractor.

_____
(Legal Name of Contractor)

_____	_____
(Signature of Authorized Signatory)	(Signature of Authorized Signatory)
_____	_____
(Print Name and Position of Authorized Signatory)	(Print Name and Position of Authorized Signatory)

SCHEDULE C-1 – STATEMENT OF DEPARTURES

1. I/We have reviewed the proposed Contract attached to the RFQ as Schedule "B". If requested by the City, I/we would be prepared to enter into that Contract, amended by the following departures (list, if any):

Section **Requested Departure(s) / Alternative(s)**

_____

_____

2. The City of Surrey requires that the successful Contractor have the following in place **before commencing the Services**:

(a) Workers' Compensation Board coverage in good standing and further, if an "Owner Operator" is involved, personal operator protection (P.O.P.) will be provided, Workers' Compensation Registration Number _____;

(b) Prime Contractor qualified coordinator is Name: _____ and Contact Number: _____;

(c) Insurance coverage for the amounts required in the proposed Contract as a minimum, naming the City as additional insured and generally in compliance with the City's sample insurance certificate form available on the City's Website at www.surrey.ca search Consultants Certificate of Insurance;

(d) City of Surrey or Intermunicipal Business License: Number _____;

(e) If the Contractor's Goods and Services are subject to GST, the Contractor's GST Number is _____; and

(f) If the Contractor is a company, the company name indicated above is registered with the Registrar of Companies in the Province of British Columbia, Canada, Incorporation Number _____.

As of the date of this Quotation, we advise that we have the ability to meet all of the above requirements **except as follows** (list, if any):

Section **Requested Departure(s) / Alternative(s)**

_____

_____

3. I/We offer the following alternates to improve the Services described in the RFQ (list, if any):

Section **Requested Departure(s) / Alternative(s)**

_____

_____

4. The Contractor acknowledges that the departures it has requested in Sections 1, 2 and 3 of this Schedule C-1 will not form part of the Contract unless and until the City agrees to

them in writing by initialling or otherwise specifically consenting in writing to be bound by any of them.

SCHEDULE C-2 – CONTRACTOR'S EXPERIENCE, REPUTATION AND RESOURCES

Contractors should provide responses to the following items, and if a particular item is inapplicable or cannot be answered, Contractors should clearly state why (use the spaces provided and/or attach additional pages, if necessary):

(i) Provide a brief description of the Contractor's current business;

(ii) Contractor's relevant experience and qualifications in delivering Services similar to those required by the RFQ;

(iii) Describe the contractor's experience in providing emergency notification system implementation services to Canadian Cities and or corporations that have similar mandates to the City of Surrey.

(iv) Contractor's demonstrated ability to provide the Services;

(v) Contractor should describe their capability, capacity and plans for developing and supporting the deliverables, as well as describe contingency plans if the primary plan is not able to meet the project needs. The objectives for this RFQ are as set out in Schedule A.

(vi) Provide how many customers you have on the West Coast including the USA and Canada. Please breakdown how many customers per location.

(vii) Using a format similar to the following, provide a summary of similar relevant contracts entered into by the Contractor in which the Contractor performed services comparable to the Services, including the jurisdiction the contract performed, the contract value, the date of performance. The City's preference is to have a minimum of three references.

Name of client's organization:	
Reference Contact Information:	**Name:**
	Phone Number:
	Email Address:
How long has the organization been a client of the Contractor?	
Provide the installation date of the comparative system, and any relevant comments.	
Description of comparative system - Please be specific and detailed.	
Information on any significant obstacles encountered and resolved for this type of Service.	

(viii) Provide the names and contact information of any customers who have switched to another vendor and system within the last three years.

(ix) Provide a detailed plan on how your service can handle a Real-World Event that affects all your clients in the same effected area. i.e. The worst-case scenario for the West Coast. What mitigation and redundancy plans do you have in place to handle all clients using your system at the same time.

(x) Contractor's financial strength (with evidence such as financial statements, bank references);

(xi) Describe any difficulties or challenges you might anticipate in providing the Services to the City and how you would plan to manage these;

(xii) Staffing Plan. Identify the key personnel who will be responsible for the Services, together with a description of the responsibilities such personnel will have in the performance of the Services and a description of the relevant experience of such personnel, using a format similar to the following:

Name: _____

Responsibility: _____

Experience: _____

_____

(xiii) Identify subcontractors, if any, the Contractor intends to use for the performance of the Services, describe the portion of the Services proposed to be subcontracted and a description of the relevant experience of the subcontractor, using a format similar to the following:

Subcontractor Name: _____

Subcontractor Services: _____

Experience: _____

SCHEDULE C-3 – CONTRACTOR'S TECHNICAL PROPOSAL (SERVICES)

Contractors should provide responses to the following items, and if a particular item is inapplicable or cannot be answered, Contractors should clearly state why (use the spaces provided and/or attach additional pages, if necessary):

(i) **Executive Summary**: Contractor should provide a brief narrative (preferably not to exceed 2 pages) that illustrates an understanding of the City's requirements and Services and describing the proposed solution. The summary should contain as little technical jargon as possible and should be oriented toward non-technical personnel. The executive summary should not include financial information;

(ii) A general description of the general approach and methodology that the Contractor would take in performing the Services including specifications and requirements;

(iii) A Work Plan. A narrative that illustrates how the Contractor will complete the scope of the Services, manage the Services, and accomplish required objectives within the City's schedule;

(iv) A description of the standards to be met by the Contractor in providing the Services;

(v) Contractor should provide in detail how its proposed technical solution meets the business and technical requirements. Please complete the attached **Functional and Technical Requirements Response Matrix, Schedule C-3-1** for the functional and technical requirements.

The following are specific questions for cloud-based solutions. In addition to the above item responses, please respond to the following items if you are proposing a Cloud Services solution.

(vi) Service Levels and Support - Cloud Services Option

(a) Describe how solution maintenance and upgrades are handled, including how maintenance and upgrades would be scheduled and communicated to the City to minimize impacts to users. For major upgrades, indicate whether the City can opt-in or out of beta testing.

(b) Describe how upgrades to your system's software, database, operating system, and/or web server components are handled. How much downtime is required for each of these types of upgrades?

(c) Describe your support plans for recovering the system in a timely manner from unplanned outages. Scenarios to address might include remote host Internet access outage, database corruption, and server software failure. Briefly describe how and how often you test your disaster recovery plans.

Please describe clearly the options available and the number of clients currently using this option. Please list your server locations that would be providing primary hosting services.

SCHEDULE C-4 – CONTRACTOR'S TECHNICAL QUOTATION (TIME SCHEDULE)

The City encourages responses that demonstrate a thorough understanding of the nature of the Services and what the Contractor must do to get the Services done properly. To this end, Contractors should provide an estimated project schedule, with major item descriptions and time indicating a commitment to perform the Services within the time specified.

As a minimum, the Contractor's Time Schedule should be in sufficient detail to specify the S breakdown structure for all tasks, deliverables and milestones, including the total number of hours of estimated work effort for the planning and implementation phases of the project (use the spaces provided and/or attach additional pages, if necessary).

ACTIVITY	**SCHEDULE**									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**

SCHEDULE C-5 – CONTRACTOR'S FINANCIAL PROPOSAL

Contractors should set out in their Quotation, the proposed fee structure (excluding GST) and provide a breakdown of the budget, including a breakdown of the estimated hours to be spent by each individual on the contractor team and the charge out hourly rate for each individual included in their Quotation.

The Fee structure should be tabulated using a financial worksheet similar in format to the attached Schedule, **Schedule C-5-1: Cloud Services.**

Additional Expenses:

The proposed Contract attached as Schedule "B" to the RFQ provides that expenses are to be included within the fee. Please indicate any expenses that would be payable in addition to the proposed fee set out above:

Payment Terms:

A cash discount of _____% will be allowed if account is paid within _____ days, or the _____ day of the month following, or net 30 days, on a best effort basis.

APPENDIX 6 – PRIVACY PROTECTION SCHEDULE

This Schedule forms part of the agreement between _____ (the "Public Body") and _____ (the "Contractor") respecting _____ (the "Agreement").

Definitions

1. In this Schedule,
   (a) "access" means disclosure by the provision of access;
   (b) "Act" means the Freedom of Information and Protection of Privacy Act (British Columbia), as amended from time to time;
   (c) "contact information" means information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual;
   (d) "personal information" means recorded information about an identifiable individual, other than contact information, collected or created by the Contractor as a result of the Agreement or any previous agreement between the Public Body and the Contractor dealing with the same subject matter as the Agreement but excluding any such information that, if this Schedule did not apply to it, would not be under the "control of a public body" within the meaning of the Act.

Purpose

2. The purpose of this Schedule is to:
   (a) enable the Public Body to comply with its statutory obligations under the Act with respect to personal information; and
   (b) ensure that, as a service provider, the Contractor is aware of and complies with its statutory obligations under the Act with respect to personal information.

Collection of personal information

3. Unless the Agreement otherwise specifies or the Public Body otherwise directs in writing, the Contractor may only collect or create personal information that is necessary for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.
4. Unless the Agreement otherwise specifies or the Public Body otherwise directs in writing, the Contractor must collect personal information directly from the individual the information is about.
5. Unless the Agreement otherwise specifies or the Public Body otherwise directs in writing, the Contractor must tell an individual from whom the Contractor collects personal information:
   (a) the purpose for collecting it;
   (b) the legal authority for collecting it; and
   (c) the title, business address and business telephone number of the person designated by the Public Body to answer questions about the Contractor's collection of personal information.

Accuracy of personal information

6. The Contractor must make every reasonable effort to ensure the accuracy and completeness of any personal information to be used by the Contractor or the Public Body to make a decision that directly affects the individual the information is about.

Requests for access to personal information

7. If the Contractor receives a request for access to personal information from a person other than the Public Body, the Contractor must promptly advise the person to make the request to the Public Body unless the Agreement expressly requires the Contractor to provide such access and, if the Public Body has advised the Contractor of the name or title and contact information of an official of the Public Body to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Correction of personal information

8. Within 5 business days of receiving a written direction from the Public Body to correct or annotate any personal information, the Contractor must annotate or correct the information in accordance with the direction.
9. When issuing a written direction under section 8, the Public Body must advise the Contractor of the date the correction request to which the direction relates was received by the Public Body in order that the Contractor may comply with section 10.
10. Within 5 business days of correcting or annotating any personal information under section 8, the Contractor must provide the corrected or annotated information to any party to whom, within one year prior to the date the correction request was made to the Public Body, the Contractor disclosed the information being corrected or annotated.
11. If the Contractor receives a request for correction of personal information from a person other than the Public Body, the Contractor must promptly advise the person to make the request to the Public Body and, if the Public Body has advised the Contractor of the name or title and contact information of an official of the Public Body to whom such requests are to be made, the Contractor must also promptly provide that official's name or title and contact information to the person making the request.

Protection of personal information

12. The Contractor must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal, including any expressly set out in the Agreement.

Storage and access to personal information

13. Unless the Public Body otherwise directs in writing, the Contractor must not store personal information outside Canada or permit access to personal information from outside Canada.

Retention of personal information

14. Unless the Agreement otherwise specifies, the Contractor must retain personal information until directed by the Public Body in writing to dispose of it or deliver it as specified in the direction.

Use of personal information

15. Unless the Public Body otherwise directs in writing, the Contractor may only use personal information if that use is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

Disclosure of personal information

16. Unless the Public Body otherwise directs in writing, the Contractor may only disclose personal information inside Canada to any person other than the Public Body if the disclosure is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.
17. Unless the Agreement otherwise specifies or the Public Body otherwise directs in writing, the Contractor must not disclose personal information outside Canada.

Notice of foreign demands for disclosure

18. In addition to any obligation the Contractor may have to provide the notification contemplated by section 30.2 of the Act, if in relation to personal information in its custody or under its control the Contractor:

(a) receives a foreign demand for disclosure;
(b) receives a request to disclose, produce or provide access that the Contractor knows or has reason to suspect is for the purpose of responding to a foreign demand for disclosure; or
(c) has reason to suspect that an unauthorized disclosure of personal information has occurred in response to a foreign demand for disclosure the Contractor must immediately notify the Public Body and, in so doing, provide the information described in section 30.2(3) of the Act. In this section, the phrases "foreign demand for disclosure" and "unauthorized disclosure of personal information" will bear the same meanings as in section 30.2 of the Act.

Notice of unauthorized disclosure

19. In addition to any obligation the Contractor may have to provide the notification contemplated by section 30.5 of the Act, if the Contractor knows that there has been an unauthorized disclosure of personal information in its custody or under its control, the Contractor must immediately notify the Public Body. In this section, the phrase "unauthorized disclosure of personal information" will bear the same meaning as in section 30.5 of the Act.

Inspection of personal information

20. In addition to any other rights of inspection the Public Body may have under the Agreement or under statute, the Public Body may, at any reasonable time and on reasonable notice to the Contractor, enter on the Contractor's premises to inspect any personal information in the possession of the Contractor or any of the Contractor's information management policies or practices relevant to its management of personal information or its compliance with this Schedule and the Contractor must permit, and provide reasonable assistance to, any such inspection.

Compliance with the Act and directions

21. The Contractor must in relation to personal information comply with:

(a) the requirements of the Act applicable to the Contractor as a service provider, including any applicable order of the commissioner under the Act; and
(b) any direction given by the Public Body under this Schedule.

22. The Contractor acknowledges that it is familiar with the requirements of the Act governing personal information that are applicable to it as a service provider.

Notice of non-compliance

23. If for any reason the Contractor does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, the Contractor must promptly notify the Public Body of the particulars of the non-compliance or anticipated non-compliance and what steps it proposes to take to address, or prevent recurrence of, the non-compliance or anticipated non-compliance.

Termination of Agreement

24. In addition to any other rights of termination which the Public Body may have under the Agreement or otherwise at law, the Public Body may, subject to any provisions in the Agreement establishing mandatory cure periods for defaults by the Contractor, terminate the Agreement by giving written notice of such termination to the Contractor, upon any failure of the Contractor to comply with this Schedule in a material respect.

Interpretation

25. In this Schedule, references to sections by number are to sections of this Schedule unless otherwise specified in this Schedule.
26. Any reference to the "Contractor" in this Schedule includes any subcontractor or agent retained by the Contractor to perform obligations under the Agreement and the Contractor must ensure that any such subcontractors and agents comply with this Schedule.
27. The obligations of the Contractor in this Schedule will survive the termination of the Agreement.
28. If a provision of the Agreement (including any direction given by the Public Body under this Schedule) conflicts with a requirement of the Act or an applicable order of the commissioner under the Act, the conflicting provision of the Agreement (or direction) will be inoperative to the extent of the conflict.
29. The Contractor must comply with the provisions of this Schedule despite any conflicting provision of this Agreement or, subject to section 30, the law of any jurisdiction outside Canada.
30. Nothing in this Schedule requires the Contractor to contravene the law of any jurisdiction outside Canada unless such contravention is required to comply with the Act.

APPENDIX 7 – CONFIDENTIALITY AGREEMENT

WHEREAS:

A. The Contractor and the City acknowledge that the process of the Contractor having access to information or software will involve the verbal, electronic, written, or other disclosure of information, and documentation to the Contractor. In this Agreement "Confidential Information" means any information, technical data, or know how, including, but not limited to that which relates to services, processes, designs, drawings, diagrams, specifications, business strategies, finances whether communicated orally or in writing, specifications and associated documentation, and any equipment, machinery, or other property all of which owned by the City.

B. The Contractor has agreed to maintain the Confidential Information as confidential and to the non-disclosure of same, all in accordance with the following terms:

THEREFORE, IN CONSIDERATION OF THE PREMISES AND OF THE MUTUAL COVENANTS SET FORTH HEREIN, THE PARTIES AGREE AS FOLLOWS:

1. The Contractor shall hold the Confidential Information in strict confidence recognizing that the Confidential Information, or any portion thereof, is comprised of highly sensitive information. The Contractor acknowledges that the disclosure or use of the Confidential Information, or any portion thereof, will cause the City substantial and irreparable harm and injury and the City shall have the right to equitable and injunctive relief to prevent the unauthorized use or disclosure, and to such damages as there are occasioned by such unauthorized use or disclosure, and the Contractor hereby consents to the granting of such equitable and injunctive relief.

2. The Contractor shall not divulge or allow disclosure of the Confidential Information, or any part thereof, to any person or entity for any purpose except as described in this Agreement, unless expressly authorized in writing to do so by the City, provided however, the Contractor may permit the limited disclosure of the Confidential Information or portion thereof only to those of the Contractor's directors, officers, employees, and sub-contractors who have a clear and *bonafide* need to know the Confidential Information, and provided further that, before the Contractor divulges or discloses any of the Confidential Information to such directors, officers, employees, and sub-contractors, the Contractor shall inform each of the said directors, officers, employees, and sub-contractors of the provisions of this Agreement and shall issue appropriate instructions to them to satisfy the obligations of the Contractor set out in this Agreement and shall, at the request of the City, cause each of the said directors, officers, employees, and sub-contractors to execute a confidentiality agreement in a form satisfactory to the City, in its sole discretion.

3. The Contractor agrees not to use any of the Confidential Information disclosed to it by the City for its own use or for any purpose except to carry out the specific purposes designated by this Agreement.

4. The Contractor shall take all necessary precautions to prevent unauthorized disclosure of the Confidential Information or any portion thereof to any person, or entity in order to prevent it from falling into the public domain or the possession of persons other than those persons authorized hereunder to have any such information, which measures shall include the highest degree of care that the Contractor utilizes to protect its own confidential information of a similar nature.

5. The Contractor shall notify the City in writing of any misuse or misappropriation of Confidential Information which may come to its attention.

6. The Contractor shall not mechanically or electronically copy or otherwise reproduce the Confidential Information, or any portion thereof, without the express advance written permission of the City, except for such copies as the Contractor may require pursuant to this Agreement in order to prepare the Report. All copies of the Confidential Information shall, upon reproduction by the Contractor, contain the same the City proprietary and confidential notices and legends that appear on the original Confidential Information provided by the City unless authorized otherwise by the City. All copies shall be returned to the City upon request.

7. The Confidential Information received by the Contractor and all formatting of the Confidential Information, including any alterations to the Confidential Information, shall remain the exclusive property of the City, and shall be delivered to the City by the Contractor forthwith upon demand by the City.

8. The Contractor acknowledges that the City is a public body subject to the *Freedom of Information and Protection of Privacy Act ("FIPPA")* and as such the Confidential Information is protected pursuant to the provisions of FIPPA. The Contractor further acknowledges that the collection, use, storage, access, and disposal of the Confidential Information shall be performed in compliance with the requirements of FIPPA. Information which is sent to the City by the Contractor in performance of this Agreement is subject to FIPPA and may be disclosed as required by FIPPA. The Contractor shall allow the City to disclose any of the information in accordance with FIPPA, and where it is alleged that disclosure of the information, or portion thereof, may cause harm to the Contractor, the Contractor shall provide details of such harm in accordance with section 21 of FIPPA.

9. The Contractor acknowledges and agrees that nothing in this Agreement does or is intended to grant any rights to the Contractor under any patent, copyright, or other proprietary right, either directly or indirectly, nor shall this Agreement grant any rights in or to the Confidential Information.

10. Disclosure of the Confidential Information to the Contractor the terms of this Agreement shall not constitute public disclosure of the Confidential Information for the purposes of section 28.2 of the *Patent Act*, R.S.C. 1985, c. p-4.

11. This Agreement shall be binding upon and for the benefit of the undersigned parties, their successors, and assigns and the Contractor hereby acknowledges that the obligations imposed on the Contractor hereunder shall survive the termination of the Contractor's dealings or engagement with the City.

12. The Contractor represents that is not now a party to, and shall not enter into any agreement or assignment in conflict with this Agreement.

13. This Agreement shall be governed and construed in accordance with the laws of the Province of British Columbia and the Contractor and the City irrevocably attorns to the exclusive jurisdiction of the courts of the Province of British Columbia to adjudicate any dispute arising out of this Agreement.

14. No provision of this Agreement shall be deemed to be waived by the City and no breach of this Agreement shall be deemed to be excused by the City unless such waiver or consent excusing such breach is in writing and duly executed by the City.

APPENDIX 8 – SERVICE LEVEL AGREEMENT

1. **Definitions**
2. **Service Levels**
3. **Availability**
4. **Planned Maintenance**
5. **Outages**
6. **Backups**
7. **Disaster Recovery**
8. **Technical Support**
9. **Service Credit**
10. **Peak Business Periods**