CITY OF SURREY
the future lives here.

REQUEST FOR PROPOSALS

Title: **Website, Virtual Exhibit – Being Punjabi**

Reference No.: 1220-030-2023-011

FOR THE ACQUISITION OF INFORMATION TECHNOLOGY SOLUTIONS

(General Services)
Issue Date: April 14, 2023

Table of Contents

REQUEST FOR PROPOSALS

1 INTRODUCTION

1.1 Purpose

The City of Surrey (the “**City**”) is interested in receiving proposals (the “**Proposal**”) from proponents (the “**Proponent**”) who have recent experience in providing a **Solution** (as defined in section 1.3) in order to manage a virtual exhibit.

This RFP is designed to provide the Proponent with the information necessary to prepare a competitive Proposal. Similarly, the RFP process is intended to also provide the City with the information it requires to select a Proponent to provide the Services. Specifically, the City is looking for a Proponent whose Solution meets or exceeds the City’s requirements as described in Schedule A.

1.2 Project Background

The Museum of Surrey has received funding from Digital Museums Canada ("DMC") to set-up a virtual exhibition on a dedicated website. They have chosen the "Being Punjabi" exhibit for this purpose. Part of this funding will be dedicated to working with an implementation partner to Plan, Design, Develop, and Deploy the website, in addition to training the team on how to maintain the website going forward.

1.3 Definitions

In this RFP 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 2.6;

“**Closing Time**” has the meaning set out in section 2.2;

“**Contract**” means a formal written contract between the City and a Preferred Proponent(s) to undertake the Services, the preferred form of which is attached as Schedule B;

“**Evaluation Team**” means the team appointed by the City;

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

“**Preferred Proponent(s)”** means the Proponent(s) selected by the Evaluation Team to enter into negotiations for a Contract;

“**Proponent**” means an entity that submits a Proposal;

“**Proposal**” means a proposal submitted in response to this RFP;

“**RFP**” means this Request for Proposals;

"**Services**" has the meaning set out in Schedule A;

"**Site**" means the place or places where the Services are to be performed; and

"**Solution**" means a Website for Virtual Exhibit - Being Punjabi and all related implementation services; and

"**Statement of Departures**" means Schedule C-1 to the form of Proposal attached as Schedule C.

2 INSTRUCTIONS TO PROPONENTS

2.1 Anticipated Solicitation Schedule

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

Solicitation Schedule	Estimated Dates
Issuance of the RFP	April 14th
Information Meeting	April 21st
Closing Date and Time	May 11th
Evaluation of Proposals	May 18th
Interviews/Demonstrations dates for Preferred Proponents only (if any)	End of May
Finalization of the Contract	Mid June
Expected "Go Live" Date	Mid 2025

The City reserves the right to modify this schedule at the City's discretion.

2.2 Closing Time and Address for Proposal Delivery

The Proponent should submit the Proposal **electronically** in a single pdf file which must be delivered by email at: purchasing@surrey.ca

on or before the following date and time

Time: **3:00 p.m., local time**
Date: **May 11, 2023**

(the "Closing Time").

Confirmation of receipt of email will be issued. Proposals that cannot be opened or viewed may be rejected. A Proponent bears all risk that the Owner's receiving computer equipment functions properly so that the Proposal is received by the Closing Time.

Note: The maximum file size the *Owner* can receive is 10Mb. If sending large email attachments, Proponents should phone [604-590-7274] to confirm receipt.

2.3 Information Meeting

An information meeting will be hosted by the City Representative to discuss the City's requirements under this RFP (the "Information Meeting"). While attendance is at the discretion of Proponents, Proponents who do not attend will be deemed to have attended the Information Meeting and to have received all of the information given at the Information Meeting. At the time of issuance of this RFP a meeting has been scheduled as follows:

When: **April 21st, 2023**

Where: **Video/Phone Conference – Microsoft Teams Meeting**

Proponents interested in participating in this Information Meeting should email their requests to purchasing@surrey.ca before (April 20th 3:00pm)

Time: **11:00am Local Time**

2.4 Late Proposals

All pages and parts of the Proposal must be received by the Closing Time. Proposals submitted after the Closing Time will not be accepted or considered.

2.5 Amendments to Proposals

Proposals may be revised by written amendment, delivered to the location set out in Section 2.2, at any time before the Closing Time but not after. An amendment should be signed by an authorized signatory of the Proponent in the same manner as provided by Section 4.2. E-mailed amendments are permitted, but such amendment should show only the change to the proposal price(s) and should not disclose the actual proposal price(s). A Proponent bears all risk that the City's equipment functions properly so as to facilitate timely delivery of any amendment.

2.6 Inquiries

All inquiries related to this RFP 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:	Sunny Kaila, Manager, Procurement Services
E-mail:	purchasing@surrey.ca
Reference:	1220-030-2023-011

Inquiries should be made no later than 7 business days before Closing Time. The City reserves the right not to respond to inquiries made within 7 business days of the Closing Time. Inquiries and responses will be recorded and may be distributed to all Proponents at the discretion of the City.

Proponents finding discrepancies or omissions in the Contract or RFP, or having doubts as to the meaning or intent of any provision, should immediately notify the City Representative. If the City determines that an amendment is required to this RFP, the City Representative will issue an addendum in accordance with section 2.7. No oral conversation will affect or modify the terms of this RFP or may be relied upon by any Proponent.

2.7 Addenda

If the City determines that an amendment is required to this RFP, 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 RFP. It is the responsibility of Proponents to check the BC Bid Website and the City Website for addenda. The only way this RFP 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 RFP or may be relied upon by any Proponent. By delivery of a Proposal, Proponent is deemed to have received, accepted and understood the entire RFP, including any and all addenda.

2.8 Examination of Contract Documents

Proponents are responsible to review all specifications, requirements, terms and conditions, insurance requirements, and other requirements herein. Proponents should be prepared to enter into a Contract substantially the same as the attached Contract. The Proponents failure to execute a Contract substantially the same as the attached Contract may result in disqualification for future solicitations for this same or similar products/services.

Submittal of a Proposal is agreement to the above condition. Proponents are to price and submit Proposals to reflect all the specifications and requirements in this RFP and terms and conditions substantially the same as those included in this RFP.

The terms and conditions set out in the Contracts are deemed to be accepted by the Proponent and incorporated into its Proposal except to the extent expressly excluded, supplemented, replaced or identified in a Proponent's Proposal (refer to Schedule C-1 – Statement of Departures). Proponents should provide reasons for any changes proposed. Proponent departures may, at the sole discretion of the City, be grounds for disqualification from further consideration in award of a contract.

The terms of a License Agreement and Support Agreement will be consistent with information provided by the Proponent in **Schedule C-3-1 – Website, Virtual Exhibit - Being Punjabi Requirements Response** of its Proposal.

The City may consider and may choose to accept some, none, or all Contract modifications that the Proponent has submitted with its Proposal.

Nothing herein prohibits the City, at its sole option, from introducing or modifying contract terms and conditions and negotiating with the Preferred Proponent to align the proposal to City needs, within the objectives of the RFP. The City has significant and critical time frames which frame this initiative; therefore, should such negotiations with the highest ranked, apparent Preferred Proponent fail to reach agreement in a timely manner as deemed by the City, the City, at its sole discretion, retains the option to terminate negotiations and continue to the next-highest ranked Proposal.

2.9 Opening of Proposals

The City intends to open Proposals in private but reserves the right to open Proposals in public at its sole discretion.

2.10 Status Inquiries

All inquiries related to the status of this RFP, including whether or not a Contract has been awarded, should be directed to the City Website and not to the City Representative.

3 COMPETITIVE SELECTION PROCESS

This Section describes the competitive selection process that the City intends to use in the selection of a Preferred Proponent or Preferred Proponents.

(a) At least three business days in advance of the demonstration the City will provide each Shortlisted Proponent with a finalized agenda the City would like to discuss;

(b) if a Shortlisted Proponent wishes to rely upon anything said or indicated at the demonstration, the Shortlisted Proponent must submit an inquiry describing the information it would like to have confirmed and request the City provide that information to the Shortlisted Proponents in written form and, if such information relates to a clarification, explanation or change to the RFP, request an addendum clarifying and/or amending the RFP;

(c) by participating in the demonstration, a Shortlisted Proponent confirms its agreement with these procedures and acknowledges that the meeting is an integral part of the competitive selection process as described in this RFP and is in the interests of all parties.

3.1 Demonstration (Shortlisted Proponents Only)

The Evaluation Team may, at its discretion, invite some or all of the Proponents to appear before the Evaluation Team to provide a presentation/demonstration of your proposed Solution.

If selected as a Shortlisted Proponent, Proponents agree to provide the Evaluation Team the opportunity to interview proposed key personnel identified by the Evaluation Team, at the option of the City. The Evaluation Team may request a Shortlisted Proponent to provide a demonstration of the Proposal as an opportunity for the Evaluation Team to ask questions and seek clarifications. This demonstration will allow Shortlisted Proponents to present their proposal and demonstrate the proposed Supplemental Security Infrastructure Software System to the Evaluation Team.

Shortlisted Proponents will be offered various dates from which to select to provide their presentation/demonstration.

The City reserves the right not to conduct demonstrations. Should the demonstrations be held, the City requires that they be led by the proposed Shortlisted Proponent’s key personnel (respective advisors, employees or representatives). The City reserves the right, to record (audio/visual) of each shortlisted Proponent’s demonstration as part of its evaluation process.

3.2 Points of Consideration for Demonstration

The following points should be considered by the Shortlisted Proponent while planning for the demonstration:

(a) All Key Personnel (as identified in Schedule C-2) of the Shortlisted Proponent should attend and actively participate in the demonstration.

(b) Shortlisted Proponents will be required to present their Proposal and demonstrate their proposed Solution to the Evaluation Team. The City Representative will schedule the time for each demonstration during the period of dates set aside for this purpose and will be indicated in the notification letter.

(c) All demonstrations will be held at Surrey City Hall on the date and time to be determined and advised by the City.

(d) Shortlisted Proponents are to provide their own hardware/software and may not have access to any other City supplied equipment. Any software/application will need to be installed on the Shortlisted Proponent’s equipment. In addition, Shortlisted Proponents are responsible for populating their demonstrations with sample data.

(e) The Solution used in the demonstration must be the same as that included in the Proposal. If certain requirements as specified in Schedule C-3-1 are met by third-party software as part of the Shortlisted Proponent’s Solution, the Shortlisted Proponent is expected to demonstrate the third party product and so indicate during the demonstration.

(f) If a Shortlisted Proponent wishes to rely upon anything said or indicated by the City at the demonstration, the Shortlisted Proponent must submit an inquiry describing the information it would like to have confirmed and request the City provide that information to the Shortlisted Proponents in written form and, if such information relates to a clarification, explanation or change to the RFP, request an addendum clarifying and/or amending the RFP.

(g) By participating in the demonstration, a Shortlisted Proponent confirms its agreement with these procedures and acknowledges that the demonstration is an integral part of the competitive selection process as described in this RFP and is in the interests of all parties.

3.3 Demonstration Schedule

The City is providing this advance, draft agenda in order for Shortlisted Proponents to adequately prepare for their demonstration. The City reserves the right to revise this draft agenda as deemed appropriate. For example, the Shortlisted Proponents may be asked to demonstrate how the Website, Virtual Exhibit - Being Punjabi satisfies the Website, Virtual Exhibit - Being Punjabi Requirements as found in Schedule A-1 the final agenda will be distributed to the Shortlisted Proponents with the Notification Letter.

Shortlisted Proponents are asked to follow the agenda and showcase the desirable functionality of the proposed Website, Virtual Exhibit - Being Punjabi Shortlisted Proponents are encouraged to highlight and discuss the unique aspects of the proposed Website, Virtual Exhibit - Being Punjabi and how their proposed Solution would benefit the City.

3.4 Shortlisted Proponents' Timeline

The dates provided in Table 1 below are approximate and are for the period up to the project "Go Live" Date.

The City reserves the right to modify the following timetable at the City's discretion.

Table 1 – Anticipated Schedule

Solicitation Schedule	Estimated Dates
Shortlisted Proponent(s) Notified	May 19th
Commencement of Demonstrations – Shortlisted Proponent(s) Only	May 24th
Shortlist Demonstrations Completed	May 31st
Selection of Preferred Proponent	June 2nd
Expected "Project Kick-off" Date	June 21st
Expected Project Go-Live Date	Mid 2025

The City reserves the right to modify this schedule at the City's discretion.

4 PROPOSAL SUBMISSION FORM AND CONTENTS

4.1 Form of Proposal

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

If a Proponent wishes to offer both a locally hosted Solution and a supplier hosted Solution, the Proponent may do so in a single Proposal.

A Proposal should include sufficient information to allow the City to verify the total cost for the project and all of the Proponent's claim of meeting the RFP's requirements. Each Proposal should respond to every request for information in the above noted schedules, whether the request requires a simple "yes" or "no" or requires a detailed narrative response. Simply repeating the RFP's requirements and agreeing to comply may be an unacceptable response.

The Proponent may include any additional information it believes is relevant. An identifiable tab sheet should precede each section of a Proposal, and each Proposal should follow the format as set out in this RFP.

4.2 Signature

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

(a) If the Proponent is a corporation then the full name of the corporation should be included, together with the names of authorized signatories. The Proposal 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 Proposal on behalf of the corporation is submitted;

(b) If the Proponent 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

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

5 EVALUATION AND SELECTION

5.1 Evaluation Team

The evaluation of Proposals will be undertaken on behalf of the City by the Evaluation Team. The Evaluation Team may consult with others including City staff members, third party consultants and references, as the Evaluation Team may in its discretion decide is required. The Evaluation Team will give a written recommendation for the selection of a Preferred Proponent or Preferred Proponents to the City.

5.2 Evaluation Criteria

The Evaluation Team will compare and evaluate all Proposals to determine the Proponent's strength and ability to provide the Website, Virtual Exhibit - Being Punjabi which is most advantageous to the City, using the following criteria:

Experience, Reputation and Resources

The Evaluation Team will consider the Proponent's responses to items in Schedule C-2.

Technical (Proposed Solution)

The Evaluation Team will consider the Proponent's responses to items in Schedule C-3 and Schedule C-4. The City will evaluate Proposals and determine whether a Proponent has met the Website, Virtual Exhibit - Being Punjabi Requirements in Schedule C-3-1. Proponents must demonstrate to the City, in the City’s sole opinion, that the Proponent meets the requirements in Schedule C-3 and Schedule C-4. Those Proponents whom the City has determined, in its sole and absolute discretion, to have met the requirements will be shortlisted.

Financial

The Evaluation Team will consider the Proponent's response to Schedule C-5.

Statement of Departures

The Evaluation Team will consider the Proponent's response to Schedule C-1.

The Evaluation Team will not be limited to the criteria referred to above, and the Evaluation Team may consider other criteria that the team identifies as relevant during the evaluation process. The Evaluation Team may apply the evaluation criteria on a comparative basis, evaluating the Proposals by comparing one Proponent's Proposal to another Proponent's Proposal. All criteria considered will be applied evenly and fairly to all Proposals.

The City’s intent is to acquire the solution that provides the best value to the City and meets or exceeds the requirements identified in this RFP.

5.3 Discrepancies in Proponent's Financial Proposal

If there are any obvious discrepancies, errors or omissions in Schedule C-5 of a Proposal (Proponent's Financial Proposal), then the City shall be entitled to make obvious corrections, but only if, and to the extent, the corrections are apparent from the Proposal 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.

5.4 Litigation

In addition to any other provision of this RFP, the City may, in its absolute discretion, reject a Proposal if the Proponent, or any officer or director of the Proponent submitting the Proposal, 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 Proponent.

In determining whether or not to reject a Proposal under this section, the City will consider whether the litigation is likely to affect the Proponent's ability to work with the City, its consultants and representatives and whether the City's experience with the Proponent indicates that there is a risk the City will incur increased staff and legal costs in the administration of the Contract if it is awarded to the Proponent.

5.5 Additional Information

The Evaluation Team may, at its discretion, request clarifications or additional information from a Proponent with respect to any Proposal, and the Evaluation Team may make such requests to only selected Proponents. The Evaluation Team may consider such clarifications or additional information in evaluating a Proposal.

5.6 Interviews

The Evaluation Team may, at its discretion, invite some or all of the Proponents to appear before the Evaluation Team to provide clarifications of their Proposals. In such event, the Evaluation Team will be entitled to consider the answers received in evaluating Proposals. Proponent management and technical personnel will be expected to participate in presentations, demonstrations and/or interviews, which will be made at no cost to the City.

All information and documents provided by the Proponents or gathered by the Evaluation Team during a presentation, demonstration or an interview may be considered by the Evaluation Team, which may revisit and re-evaluate the Proponent's Proposal or ranking on the basis of such information and documents.

5.7 Multiple Preferred Proponents

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 Preferred Proponents 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 RFP and the basis of Proposals.

In addition to any other provision of this RFP, Proposals may be evaluated 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 Proponents.

5.8 Negotiation of Contract and Award

If the City selects a Preferred Proponent or Preferred Proponents, then it may:

(a) enter into a Contract with the Preferred Proponent(s); or

(b) enter into discussions with the Preferred Proponent(s) to attempt to finalize the terms of the Contract(s) (and, if applicable, a License Agreement and Support Agreement as described in section 2.8), including financial terms, and such discussions may include:

   (1) clarification of any outstanding issues arising from the Preferred Proponent's Proposal;

   (2) negotiation of amendments to the departures to the draft Contract, if any, proposed by the Preferred Proponent as set in Schedule C-1 to the Preferred Proponent's Proposal; and

   (3) negotiation of amendments to the Preferred Proponent's price(s) as set out in Schedule C-5 to the Preferred Proponent's Proposal and/or scope of Services if:

      (A) the Preferred Proponent's financial Proposal exceeds the City's approved budget, or

      (B) the City reasonably concludes the Preferred Proponent's financial proposal includes a price(s) that is unbalanced, or

      (C) a knowledgeable third party would judge that the Preferred Proponent's price(s) materially exceed a fair market price(s) for services similar to the Services offered by the Preferred Proponent as described in the Preferred Proponent's Proposal; or

(c) if at any time the City reasonably forms the opinion that a mutually acceptable agreement is not likely to be reached within a reasonable time, give the Preferred Proponent(s) written notice to terminate discussions, in which event the City may then either open discussions with another Proponent or terminate this RFP and retain or obtain the Services in some other manner.

6 GENERAL CONDITIONS

6.1 No City Obligation

This RFP is not a tender and does not commit the City in any way to select a Preferred Proponent, 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 Proposals, and to terminate this RFP process.

6.2 Proponent’s Expenses

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

6.3 No Contract

By submitting a Proposal and participating in the process as outlined in this RFP, Proponents expressly agree that no contract of any kind is formed under, or arises from, this RFP, prior to the signing of a formal written Contract.

6.4 Conflict of Interest

A Proponent shall disclose in its Proposal 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.

6.5 Solicitation of Council Members, City Staff and City Consultants

Proponents and their agents will not contact any member of the City Council, City staff or City consultants with respect to this RFP, 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 RFP and which could be viewed as one Proponent attempting to seeks an unfair advantage over other Proponents.

6.6 Confidentiality

All submissions become the property of the City and will not be returned to the Proponent. All submissions will be held in confidence by the City unless otherwise required by law. Proponents 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.

6.7 Reservation of Rights

The City reserves the right, in its sole and absolute discretion, to:

(a) amend the scope of Services, modify, cancel or suspend the competitive selection process at any time for any reason;
(b) accept or reject any Proposal, based on the Evaluation Criteria;
(c) waive a defect or irregularity in a Proposals, and accept that Proposal;
(d) reject or disqualify or not accept any or all Proposals, without any obligation compensation or reimbursement to any Proponent or any of its team members;
(e) re-advertise for new Proposals, or enter into negotiations for the Services or for Services of a similar nature;
(f) make any changes to the terms of the business opportunity described in this RFP;
(g) negotiate any and all aspects of Proposals; and
(h) extend, from time to time, and date, time period or deadline provided in this RFP, upon written notice to all Proponents.

6.8 Acceptance of Proposals

Notwithstanding anything to the contrary contained in the RFP or any other document, material or communication:

(a) The City will not necessarily accept the Proposal with the lowest Proposal Price, or any Proposal, and the City reserves the right to reject any and all Proposals at any time, or cancel the RFP process, without further explanation and to accept any Proposal the City considers to be in any way advantageous to it. The City's acceptance of any Proposal is contingent on having sufficient funding for the Solution and a Contract with a Proponent. Proposals containing qualifications will be considered to be non-conforming Proposals in that they will fail to conform to the requirements of the RFP documents and on that basis they may be disqualified or rejected. Nevertheless, the City may waive any non-compliance with the requirements of the RFP documents, specifications or any conditions, including, without limitation, the timing of delivery of anything required by these RFP documents, and the City, at its discretion, may consider non-conforming Proposals and accept a non-conforming Proposal.

(b) Where the City is of the view, in its sole discretion, that there is an ambiguity or other discrepancy which cannot be discerned or resolved from examining the contents of the Proposal, then whether or not such an ambiguity or discrepancy actually exists on the face of the Proposal, the City may, prior to Contract award, solicit clarification from the Proponent or accept clarification from the Proponent on any aspect of its Proposal. Such clarification may include the acceptance of any further documents or information which will then form part of the Proposal. The soliciting or accepting of such clarification (whether or not solicited) by the City will be without any duty or obligation on the City to advise any other Proponents or to allow them to vary their Proposal Prices as a result of the acceptance of clarification from any one or more Proponents and the City will have no liability to any other Proponent(s) as a result of such acceptance of clarification.

(c) If the City considers that all Proposals are priced too high, it may reject them all.

(d) The City, prior to awarding of any Contract, may negotiate with the Proponent presenting the lowest priced Proposal, or any Proponent, for changes in the Solution, the materials, the specifications or any conditions, without having any duty or obligation to advise any other Proponents or to allow them to modify their Proposal, and the City will have no liability to any Proponent as a result of such negotiations or modifications.

(e) The City and its representatives, agents, consultants and advisors will not be liable to any Proponent for any claims, whether for costs, expenses, losses, damages, or loss of anticipated profits, or for any other matter whatsoever, incurred by a Proponent in preparing and submitting a Proposal, or participating in negotiations for a final Contract, or other activity related to or arising out of this RFP, including in the event the City accepts a non-compliant Proposal or otherwise breaches the terms of this RFP.

(f) A pre-award meeting may be conducted with the preferred Proponent prior to award to confirm project details and expectations of the City.

(g) Proponents are solely responsible for their own expenses in preparing and submitting a Proposal, and for any meetings, negotiations or discussions with the City, or its representatives and consultants, relating to or arising from the RFP. The City will not be liable to any Proponent for any claims, whether for costs, expenses, losses or damages, or loss of anticipated profits, incurred by the

Proponent in preparing and submitting a Proposal, or participating in negotiations for a contract, or other activity related to or arising out of this RFP.

SCHEDULE A – SCOPE OF SERVICES

PROJECT TITLE: Website, Virtual Exhibit - Being Punjabi

1. SCOPE OF SERVICES

The Museum of Surrey has received funding from Digital Museums Canada ("DMC") to set-up a virtual exhibition on a dedicated website. They have chosen the "Being Punjabi" exhibit for this purpose. Part of this funding will be dedicated to working with an implementation partner to Plan, Design, Develop, and Deploy the website, in addition to training the team on how to maintain the website going forward.

The overall goals of the website are:

- Increase accessibility to reach and engage with a wider audience.
- Leverage technology to increase engagement – allowing audience to interact and view items in different ways.
- Provide the team a platform to update and edit and customize as needed.

1.1 Current State

The temporary exhibition “Being Punjabi” was presented at the Museum of Surrey in 2019-2020 and was a tribute to Punjabi community members who came forward to share their story, inviting us to celebrate Surrey’s diversity and to challenge assumptions we make about each other.

Currently there is no website or content created to represent the “Being Punjabi” exhibit, the website development and overall user experience would need to be built from the ground up.

1.2 Target State for the Website

In addition to the full list of detailed requirements outlined in Schedule A1, the preferred target state for the website is one that is:

- Designed with the input and collaboration of the City of Surrey team;
- Developed on Drupal using best practice coding standards;
- Hosted on the City of Surrey’ Acquia hosting environment;
- Trilingual website functionality is required (English, French, Punjabi);
- Accessible and functional from all current mobile devices.

Ideal candidates would preferably also have experience with:

- Digital Museum of Canada (DMC) projects
- Azure AD integrations using SimpleSAMLphp

1.3 Target State for Hosting

The intention is to have the new website hosted on the Acquia Hosting platform. The City of Surrey currently has Acquia in place and has several websites already hosted on

Acquia. The selected proponent would preferably have experience with website deployments and be able to work with the City's current Drupal maintenance vendor.

The hosting-based requirements detailed in Schedule C-3 are managed by Acquia. If the Proponent recommends an alternate hosting solution, then the requirements detailed in Schedule C-3 would be applicable to said solution.

1.4 Target State for Maintenance and Support

While ongoing maintenance and support of the website will be handled by the City's current Drupal maintenance vendor. The selected proponent would be required to supply full 'as built' technical documentation of all modules and systems to be consumed by future developers and administrators. Training materials for City super users should also be provided.

2. FUNCTIONAL AND TECHNICAL REQUIREMENTS

The requirements for this RFP are divisible into three general categories: non-functional requirements, DMC Technical Requirements and security requirements (the **"Website, Virtual Exhibit - Being Punjabi Requirements**"), all as described and embedded in Schedule A-1**.** The security requirements are further divisible into general, web application, mobile application, and cloud.

Proponents' Proposals will be evaluated based upon the suitability of their proposed Solution(s) in relation to the Solution Requirements. The functional requirements generally list the City's desired/preferred or required general Website, Virtual Exhibit - Being Punjabi functionality. The technical requirements list the City's desired or required general Website, Virtual Exhibit - Being Punjabi functionality in areas such as integration, user interface, analytics and reporting, and others. Most of the functional and technical requirements are preferred or highly preferred by the City, and Proponents will be evaluated on their ability to meet those requirements.

As part of their Proposal, Proponents should submit Schedule C-3-1 (Website, Virtual Exhibit - Being Punjabi Requirements Response), which is available as a separate attachment to this RFP, after filling-in the spreadsheet's two right-most columns. Specifically, the Proponent should indicate if their Solution complies with each requirement by selecting the appropriate response code in the response code field, and also provide a description in the comments field that explains how their Solution meets each requirement.

Some of the Website, Virtual Exhibit - Being Punjabi Requirements are identified as mandatory, and must be met for the Proponent's Solution to be considered.

2.1 Deployment

The City makes use of three environments for solutions development, each of which fulfils a specific need to control the quality and stability of our environments as a whole. It is expected that the Proponent follow the City's development process and adhere to using the prescribed environments.

Development Environment

The Proponent will develop code that can be deployed from our code repository to the Development Environment. Code will be unit tested against defined test cases to ensure quality prior to promotion to the test environment.

Test Environment

The Proponent is responsible for deploying to the Test Environment. This environment will closely resemble what the desired production environment will entail. The City's staff will perform their testing here. Review demonstrations will also be performed from this environment. Deployments to the test environment must be automated through the deployment pipeline. Any issues encountered here must be resolved prior to production deployment.

Production Environment

The deployment to production must be approved by City staff. The Proponent is responsible for deploying to the Production Environment. Documentation must be provided by the Proponent in order to allow City staff to perform the production deployment as well as test deploy the solution to any other test environment.

2.2 Source Code Management

The City currently uses GitHub as our code repository. The Proponent will consistently commit the code to the GitHub repository which the City will have access to throughout the project. All final production code must reside in the City's GitHub source code repository.

A Continuous Integration/Continuous Deployment (CI/CD) pipeline will be put in place by the Proponent to automate build, test, and deployment of our website.

The City must be able to redeploy the website from this source code repository. All configuration documentation, workflow documentation, CI/CD documentation, training documentation and overall knowledge on how to redeploy the website must be made available to the City.

2.3 Product Handover

The Proponent will provide detailed documentation covering the following areas:

- Technical design/decisions – code level documentation for City staff to utilize for ongoing operational support, as well as for future enhancements;
- Operational support – environment level documentation for City staff to utilize for ongoing operational support; and
- Testing – documentation outlining the test cases and requirements satisfied.

2.4 Knowledge Transfer

The Proponent will provide knowledge transfer sessions where the documentation can be reviewed, and further questions and answers provided. Workshops will be provided for the City's teams to facilitate successful product handover.

The City reserves the right to make video and/or audio tape recordings of any and all training sessions, whether held at the City or the Contractor’s site, or via teleconference. Use of such training recordings shall be strictly for City staff training purposes.

- END OF PAGE -

SCHEDULE A-1 – FUNCTIONAL AND TECHNICAL REQUIREMENTS

For greater certainty, the requirements listed in **Schedule A-1 (Website, Virtual Exhibit - Being Punjabi Requirements)** and **Schedule C-3-1 (Website, Virtual Exhibit - Being Punjabi Requirements Response)** are identical. The only difference between the two Schedules is that Schedule C-3-1 contains two additional columns for the Proponent to enter information regarding its own Proposal.

Schedule A-1 may be viewed and/or downloaded from the City of Surrey's Managed File Transfer Service (MFT):

Hostname:	https://mft.surrey.ca
Logon ID	surrey bid
Password:	Welcome

Locate Folder	1220-030-2023-011

FUNCTIONAL AND TECHNICAL REQUIREMENTS

Non-Functional Requirements					
Req. #	**Requirement**	**Elaboration**	**Category**	**Theme**	**Level Of Need**
Planning and Technical Design					
1000	Develop website using the Drupal 10	Coded with Drupal best practises, coding standards, and forward compatibility to be robust for 5 years post launch	Development	Drupal	Mandatory
1001	Ability to leverage Drupal 10 modules and features to support multiple page types	Examples: Homepage, landing pages, basic pages, event pages, news pages, location pages, search/search results.	Development	Drupal	Mandatory
Project management and processes					
1002	Demos	Vendors must deliver demos showing implementation progress for the COS team throughout the development lifecycle if requested.			Mandatory
1003	Requirement traceability	Vendors must use Project Management practices to track feature development and tasks back to core requirements, to demonstrate progress and completion			Mandatory
Sign Off Requirements					
1004	Provide documentation outlining process for building the site and as built	Develop and maintain technical documentation of the site for other or future developers and administrators.	Development	Documentation	Highly Desirable
1005	Requirements sign off	All requirements must be approved, signed and tracked in a central location before considered complete			Mandatory
1006	Documentation Required for every content type, block and feature	Detailed specification of each component outlining description, configuration, features, limitations and what can be customized. Expectation is to have an end state version be presented in an excel format such as this: https://docs.google.com/spreadsheets/d/1pVQNyE5Rqhdnzk-6dHN5nnH_FsGfjub2_bzQF5MewSs/edit#gid=0	Development	Documentation	Mandatory

1007	User documentation for main tasks performed by the Web Team should be provided upon product delivery.	Additional training materials may include user manuals, video tutorials, etc .			Highly Desirable
1008	Testing as different users roles	The contractor will walk through using any new feature, block, or content type in all defined user roles (ie. Content Author, Editor, etc.) before handing it over to the COS team to ensure the editor view works properly.	QA	Testing	Highly Desirable
1009	Proponent is responsible to work with project team to develop UX/UI design and layouts	Design documents that are a visual representation of desktop and/or mobile experience-Eg., wireframes, moodboards, style guides, user flow etc.	Design	Drupal	Mandatory
1010	Proponent is responsible for implementing the approved design in Drupal 10 to proper Drupal standards and best practices.	This includes implementing any of the content structures, views, templates, taxonomies and any other modules needed to fully realize the required functionality based on the approved design/UX and site content.	Development	Drupal	Mandatory
1011	Proponent will be required to work with CoS Drupal Maintenance team, submitting code through our established development CI/CD workflows which will include code reviews		Development	Drupal	Mandatory
1012	Proponent is responsible for delivering a detailed list of enhancements.	This should include features and how it should behave.: Eg., interactive timelines, interactive maps, slideshows, light boxes, parallax scrolling, full-screen background videos, games, forms, animation etc. Specify which technologies or products will be used to implement the feature.	Development	Drupal	Mandatory
1013	Proponent must provide documentation during the design phase that describes how technical solution meet DMC accessibility and language requirements		Design	Drupal	Mandatory

Technical Requirements					
Req. #	Requirement	Elaboration	Category	Theme	Level of Need
2000	The Website must meet the AA compliance level of World Wide Web Consortium’s (W3C) Web Content Accessibility Guidelines 2.1 (WCAG 2.1)		Development	Accessibility	Mandatory
2001	Website MUST comply with all success criteria up to and including WCAG 2.1 Level AA, related to the perceivable principle.		Development	Accessibility	Mandatory
2002	Text alternatives MUST be provided for any non-text content.	So that it can be changed into other needed forms, such as large print, braille, speech, symbols, or simpler language.	Development	Accessibility	Mandatory
2003	Text or static content for time-based multimedia (such as video and audio) MUST be provided.	When audio or video can not be played, reasonable fallbacks must be provided.	Development	Accessibility	Mandatory
2004	All audio and video must meet the accessibility requirements		Development	Accessibility	Mandatory
2005	The visual presentation of text and images of text MUST meet the minimum requirements for colour contrast as per WCAG's 1.4.3 Contrast (Minimum) success criterion.		Design	Accessibility	Mandatory
2006	Information, structure, and relationships SHOULD be conveyed through presentation and coded accordingly.	When the sequence in which content is presented affects its meaning, a correct reading sequence SHOULD be in place.	Development	Accessibility	Highly Desirable

2007	User interface components and navigation MUST be operable. Website MUST comply with all success criteria up to and including WCAG 2.1 Level AA, related to the operable principle.		Development	Accessibility	Mandatory
2008	All functionality MUST be keyboard accessible.	This requirement includes video and audio controls, navigational aids, and the means to fill out online forms.	Development	Accessibility	Mandatory
2009	Any keyboard operable user interface MUST have a mode of operation where the keyboard focus indicator is clearly visible and consistent from browser to browser.	The default focus indicator built into browsers SHOULD NOT be relied upon.	Development	Accessibility	Mandatory
2010	add links and targets to bypass blocks of content and navigation through the various fields, objects, and controls on the page MUST be presented in a logical order. This order MUST remain consistent and usable when keyboard tabulation order is used.	To help users navigate, find content, and determine where they are in the website.	Design/Development	Accessibility	Highly Desirable
2011	User interface operation and information MUST be understandable. Website MUST comply with all success criteria up to and including WCAG 2.1 Level AA, related to the understandable principle.		Development	Accessibility	Mandatory

2012	Web pages MUST appear and operate in predictable ways by providing consistent navigation and identification.	The site MUST NOT open multiple windows or pop-ups, create periodically auto-refreshing pages, or redirect pages automatically. When the state of the page changes, the URL MUST be adjusted so that each location is unique and identifiable.	Development	Accessibility	Mandatory
2013	Semantic markup (<h1 />, <h2 />, <em />, <abbr />, etc.) MUST only be used to convey meaning (for example, to convey the semantics) of content, rather than to add visual style.		Development	Accessibility	Mandatory
2014	Text MUST be readable and understandable.	This is achieved by identifying the language the page is in, identifying text displayed in another language, and providing the expanded form or meaning of abbreviation/acronyms. Note: This is a WCAG 2.1 Level AAA item that DMC is including.	Design	Accessibility	Mandatory
2015	Web pages MUST appear and operate in predictable ways by providing consistent navigation and identification. Form fields MUST have clear labels and instructions.	Examples: On mobile devices, the site MUST NOT open multiple windows or pop-ups, create periodically auto-refreshing pages, or redirect pages automatically.	Design/Development	Accessibility	Mandatory
2016	Mechanisms MUST be put in place to ensure form error prevention, identification and suggestion for recovery and correction.		Development	Accessibility	Mandatory
2017	Website must comply with all success criteria up to and including WCAG 2.1 Level AA, related to the robust principle.	Content MUST be robust enough that it can be interpreted reliably by a wide variety of user agents, including assistive technologies.	Development	Accessibility	Mandatory

2018	Website MUST be compatible with Mac, Windows, iOS and Android.		Development	Devices	Mandatory
2019	Website MUST be identically functional and compatible on top market share iOS and Android phones dating back at least 2 years from present date.		Development	Devices	Mandatory
2020	Website MUST be mostly functional and compatible on top market share iOS and Android phones dating back 4 years or more from present date.		Development	Devices	Mandatory
2021	Website MUST be identically functional and compatible on top market share browsers (Chrome, Firefox, Safari, Edge) dating back at least 2 years from latest stable version.		Development	Browser	Mandatory
2022	Website MUST be mostly functional and compatible on top market share browsers (Chrome, Firefox, Safari, Edge) dating back 4 years from latest stable version.		Development	Browser	Mandatory
2023	Screen reader comprehension MUST be tested using one of the most common screen reader and browser combinations: VoiceOver and Safari if on a Mac, and JAWS with Chrome or NVDA with Firefox if on Windows.		Testing/QA	Accessibility-Translation	Highly Desirable
2024	Markup elements MUST have start and end tags and MUST be nested according to their specifications. They MUST NOT contain duplicate	To maximize compatibility with current and future user agents. These characteristics can be validated using	Development		Mandatory

	attributes, and all IDs MUST be unique.	the W3 validator at: http://validator.w3.org/.			
2025	Website MUST be developed using responsive web design principles, meaning there is a single version of the website with a fluid presentation layer that adapts to any screen size.		Development	Front-End	Mandatory
2026	Technologies MUST be chosen to ensure that the content of the website is available to the greatest number of visitors regardless of technical, physical, or cognitive impairment.		Development	Accessibility	Highly Desirable
2027	The core of every website MUST be a base HTML version that presents all content in a simplified format, providing a basic level of user experience in all browsers.	The goal and idea behind progressive enhancement, is that no matter what technology layer(s) are removed (WebGL, JavaScript, CSS), pages MUST remain comprehensible and functional, although to a lesser degree.	Development	Front-End	Highly Desirable
2028	The website must be built using progressive enhancement methodology with unobtrusive JavaScript	Unobtrusive JavaScript is the process or principle of JavaScript being used to complement and enhance the base HTML layer. It's the notion that using JavaScript MUST NOT be at the subjugation or dismissal of the underlying HTML and CSS layers.	Development	Front-End	Highly Desirable
2029	Website MUST use the Transport Layer Security (TLS) protocol throughout the site.		Development	Security	Mandatory
2030	Website MUST use the TLS protocol when users are required to input a username and password.		Development	Security	Mandatory

2031	On pages using TLS, all hyperlinks to pages that do not use this protocol MUST use relative URLs once the user has sent a request to stop using TLS (for example, logout after opening a session).		Development	Security	Mandatory
2032	Website be developed in a way that maximizes SEO	• Search engine findability and crawlability of the website's main pages • Shareability of the website's main pages on social media • How well the website's main pages display in search engine results pages • Every page MUST include a unique HTML document title and meta description	Development	SEO	Mandatory
2033	Website MUST include a home page for each language version of the product.		DMC Content	Translation	Mandatory
2034	Website MUST include a full copyright statement identifying all rights holders for each language version.		DMC Content	Translation	Mandatory
2035	Website MUST include a page with full credits for each language version. The credits page statement MUST acknowledge the financial participation of the Government of Canada		DMC Content	Translation/Content	Mandatory
2036	Website MUST include a simple HTML feedback form in each respective official language.	The feedback form MUST be configured to send an email to the organization responsible for the website	Development	Translation	Mandatory

2037	The feedback form MUST be organized in a logical order.	Requirements for the form are as follows: • The form MUST include an email field, comments text area, and a submission button followed by a clear button. • Labels MUST be associated with their controls, and logical grouping of form elements MUST be contained with the <field set /> with a <legend /> for each group. • Forms MUST be accessible; that means, functional and understandable via keyboard only or keyboard accompanied with a screen reader. Users MUST be advised of the privacy issues associated with sending feedback through email	Design	Usability	Mandatory
2038	Website MUST include a sitemap page for each language version.	English, French and Punjabi	Development	Translation	Mandatory
2039	Website MUST be developed in three languages, English and French and Punjabi	• All content MUST be translated and available in both languages • All webpages MUST have distinct URLs in each respective language • It is NOT sufficient to merely link to the opposing language's home page • Each page MUST have a language toggle link • Selecting the language toggle MUST return the same page and content but in the opposing language	Development	Translation	Mandatory

2040	Every page MUST distinctively include the DMC logo.	The logo MUST appear in the top right-hand corner of each page with adequate considerations made so that it is distinct (visually and programmatically) from other elements surrounding it. Any alternative to this requirement MUST be agreed upon by both parties.	DMC Content	Front-End	Mandatory
2041	Every page of the website MUST include Google Analytics tracking code used to collect visitor data.		Development	Analytics	Mandatory
2042	Webpages MUST load reasonably quickly with page load times (0.5-1 second).		Development	Performance	Mandatory
2043	Mobile views need to be optimized for reasonable performance and data load.	In addition, the size of content and downloads, the number of calls to the server, as well as page refreshes MUST be reduced as much as possible.	Development	Performance	Highly Desirable
2044	File sizes for all file types MUST be optimized.	In particular, to produce the final image, audio and video files, settings MUST be used to optimize file size down to something reasonable for web consumption but NOT at the sacrifice of visibly degraded quality.	Development	Performance	Mandatory
2045	The site MUST be password protected	During website development, search engines and the general public must not access the site.	Development	Security	Mandatory
2046	Password protection MUST be done at the server level, rather than programmatically.		Development	Security	Mandatory
2047	Website must support a variety of content formats (i.e., images, videos, audio clips, and text)	Approx. 50-100 Images Approx. 5-10 Videos	Development	Content	Mandatory

		Approx. 3-6 Audio Clips Unlimited text			
2048	Website must let the community user to submit story feedback forms - [Text and Images]	Form provided for users to submit their stories. Form to allow submission of user contact info, text and media. Image media upload of jpg files no larger than 2 MB Text documents – pdf	Development	Content	Mandatory
2049	Feedback form must be protected from spam/hostile posting		Development	Security	Mandatory
2050	Ability for the website to let the community user to submit story feedback forms-[Videos]	Audio clips – either .MP3 or .MP4 Video media – as link to streaming service (e.g. YouTube or Vimeo)	Development	Content	Highly Desirable
2051	User contribution display, submissions require a curation process for museum staff to approve or finalize content before displayed live on the site		Development	Content	Highly Desirable
2052	User content to be displayed in listing for browsing submitted stories and in view that displays all details/content submitted		Development	Content	Highly Desirable
2053	Must have the ability to create an interactive timeline feature using images and text	(e.g., click on a spot in the timeline and information regarding that time will appear)	Development	Content	Mandatory
2054	Ability to include video and/or audio clips in the interactive timeline feature	(e.g., click on a spot in the timeline and information regarding that time will appear)	Development	Content	Highly Desirable

Service Level & Support Requirements					
Req. #	**Requirement**	**Elaboration**	**Category**	**Theme**	**Level of Need**
3000	We consider system outages as		Cloud	Availability	Preferred
	1) a complete inability to use the solution, or			Uptime	Preferred
	2) a reoccurring, temporary inability to use the solution, or			Planned Maintenance	Preferred
	3) an inability to use the features and functions integral to the solution's core business purpose.			Planned Maintenance	Preferred
	Your solution's availability criteria should meet this definition. If not, please specify any departure.			Performance	Preferred
3001	For a Cloud Solution, the uptime should meet or exceed 99.99% per year.		SLA	Access to City Data	Preferred
3002	For a Cloud Solution, The City must be notified 4 weeks in advance of any planned or unplanned maintenance the application needs within the working hours define in Req :3004		Application	Access to City Data	Mandatory
3004	For a Cloud Solution, The Application response latency over the Internet should be less than 120ms.	The users located on the West Coast need good Application performance when the Cloud datacenter is on the East coast.	Application	Service Credit	Preferred
3005	Should support data portability (the ability to move City Data to another provider at the City's discretion).		Cloud	Support	Preferred
3006	Must provide the City with a Certificate of Destruction when Data is no longer required.		Cloud	Support	Mandatory

3008	For SLA not met during Working Hours, the City requires Service Credits to be issued.	If the proponent fails to meet a SLA requirement and the application is down during working hours, the City must be issued Service Credits to recompense the City further spend with the proponent. These could be used against on-going services, professional services or customisations that the City would normally pay for.	Service	Support	Mandatory
3009	For a Cloud Solution, the proponent must provide Application Support 24/7. This includes the main Application functionality, Integrations and service outages.	Support Staff at the City need to be able to create incidents and have them tracked to resolution. A system should be in place to a) provide tiered support to allowing for escalation.	Application	Performance	Highly Desirable
		b) provide support response times and expected resolution times for each incident.		Enhancements	Highly Desirable
3010	Access to a ticket management system for triage and communication;	Support Staff at the City need to be able to create incidents and have them tracked to resolution. A system should be in place to	Service	Consultation	Highly Desirable
		a) provide tiered support to allowing for escalation.		Consultation	Highly Desirable
		b) provide support response times and expected resolution times for critical and urgent incidents		Support	Highly Desirable
		c) provide means for City staff to comment on existing tickets		Support	Desirable
		d) include notification system to alert required City staff of changes in ticket details, status and comments		Support	Desirable
3011	Monitor and track Drupal releases	Vendor will be responsible for monitoring release notifications from Drupal, and will be required to manage application updates in a proactive manner.	Application	Support	Mandatory

3012	Manage and apply Drupal Core and Module security updates and patches	All releases that include a security fix must be applied to the website within 7 days.	Application	Support	Mandatory
3013	Manage and apply Drupal Core and Module maintenance releases	Track, manage and implement all non-security updates to both Drupal Core and installed module on minimum of monthly schedule.	Application	Support	Mandatory
3014	Provide support and assistance to resolve site performance issues	Vendor be required to investigation and assist in resolving performance issues with hosting provider. This could involve setting up application performance tests, investigating potential application adjustments for performance optimization or adjusting system configuration settings	Application	Performance	Highly Desirable
3015	Ability to take on requests for small to mid-size projects for feature enhancements and functionality improvements	Vendor should be able to support small to mid-size feature enhancment requests for any aspect of Drupal site to change in content structure, logic and functionality both at front-end theme layer and administration, either as additional service or to an agreement of a set number of hours for enhancements per month	Application	Enhancements	Highly Desirable
3016	Provide consultation and advice application enhancements	Provide consultation and advice for Drupal specific features and improvement as required, particularly where it involves custom integration with other applications and systems	Application	Consultation	Highly Desirable
3017	Provide consultation and advice on user-experience enhancements	Advise the business stakeholders and the user experience team of applicable technical options, limitations and restrictions related to front end web development;	Application	Consultation	Highly Desirable
3018	Backup and recovery, disaster recovery plan	Vendor should be able provide solution for backup and recovery of application data, files, information in case of catastrophic loss	Application	Support	Highly Desirable

3019	Provide training for feature enhancements or best practices	Vendor should be able to provide training and demonstration of feature enhancements or change in functionality to ensure that City staff are using the application properly and for best results.	Application	Support	Desirable
3020	Provide updates manual and technical documentation	Provide updated technical documentation and manuals to reflect feature enhancements or system changes	Documentation	Support	Desirable

GENERAL SECURITY REQUIREMENTS

Access Control

Req. #	Category	Requirement	Level of Need
4000	User Authentication / Secure Login	System access must be controlled by a secure login procedure the authenticates a users identity.	Mandatory
4001	Active Directory Integration	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.	Mandatory
4002	Roles Based Access / Authorization	The system must support roles based (or group based) access control.	Mandatory
4003	Password Management	The system must support enforcing the City's password policy. Ideally, the system can integrate with Active Directory and leverage Kerberos for authentication.	Mandatory
4004	Multi-Factor Authentication (MFA)	The system should support the use of the City's Multi-Factor authentication solution (AzureAD MFA) for access from untrusted locations.	Preferred
4005	User Access Provisioning	The system should support automatic user provisioning/de-provisioning. Note: This requirement can be ignored if AD integration is possible.	Preferred
4006	Privileged Account Management	The system should support integration with leading Privileged Identity Management solutions.	Desired
4007	Password Encryption	Any passwords stored in the database, the application, or configuration files must be encrypted.	Mandatory

Encryption

Req. #	Control Area	Requirement	Level of Need
4008	Encryption of Data in Transit	The system must support the encryption of City data while in transit.	Mandatory if Cloud, otherwise Preferred
4009	Encryption of Data at Rest	The system must support the encryption of City data while at rest.	Mandatory if Cloud, otherwise Preferred
4010	Encryption Protocols	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.	Preferred

Auditing and Logging

Req. #	Control Area	Requirement	Level of Need
4011	Security Event Logging	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.	Mandatory
4012	Log Protection	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.	Preferred
4013	Auditing	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.	Mandatory

Vulnerability Management

Req. #	Control Area	Requirement	Level of Need
4014	Patch Management	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.	Preferred
4015	Malware protection	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.	Preferred

WEB APP SECURITY REQUIREMENTS			
Req. #	Category	Requirement	Level of Need
5000	Web Authentication	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).	Preferred
5001	Session Management	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.	Preferred
5002	Web Access Control	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.	Preferred
5003	Web Input Validation	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	Preferred
5004	Web Cryptography at Rest	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.	Preferred
5005	Web Error Handling and Logging	All web applications should fail securely, and not reveal any sensitive or application configuration information in error messages.	Preferred

5006	Web Data Protection	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.	Preferred
5007	Web Service Security	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	Preferred

CLOUD SECURITY REQUIREMENTS

Req. #	Category	Requirement	Level of Need
7000	Application & Interface Security Application Security	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.	Preferred
7001	Application & Interface Security Customer Access Requirements	Prior to granting a customer access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	Mandatory
7002	Application & Interface Security Data Integrity	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.	Preferred
7003	Application & Interface Security Data Security / Integrity	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.	Preferred
7004	Audit Assurance & Compliance Audit Planning	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.	Preferred
7005	Audit Assurance & Compliance Independent Audits	Independent reviews and assessments must be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	Mandatory

7006	Audit Assurance & Compliance Information System Regulatory Mapping	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.	Preferred
7007	Business Continuity Management & Operational Resilience Business Continuity Planning	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	Preferred
7008	Business Continuity Management & Operational Resilience Business Continuity Testing	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.	Mandatory
7009	Business Continuity Management & Operational Resilience Datacenter Utilities / Environmental Conditions	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.	Preferred
7010	Business Continuity Management & Operational Resilience Documentation	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	Preferred
7011	Business Continuity Management &	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm,	Mandatory

	Operational Resilience Environmental Risks	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.	
7012	Business Continuity Management & Operational Resilience Equipment Location	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.	Preferred
7013	Business Continuity Management & Operational Resilience Equipment Maintenance	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.	Preferred
7014	Business Continuity Management & Operational Resilience Equipment Power Failures	Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific Business Impact Assessment	Preferred
7015	Business Continuity Management & Operational Resilience Impact Analysis	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	Preferred
7016	Business Continuity Management & Operational Resilience Policy	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	Preferred

		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.	
7017	Business Continuity Management & Operational Resilience Retention Policy	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.	Preferred
7018	Change Control & Configuration Management New Development / Acquisition	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.	Preferred
7019	Change Control & Configuration Management Outsourced Development	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).	Preferred
7020	Change Control & Configuration Management Quality Testing	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.	Preferred
7021	Change Control & Configuration Management Unauthorized Software Installations	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.	Preferred
7022	Change Control & Configuration Management Production Changes	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	Preferred

		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.	
7023	Data Security & Information Lifecycle Management Classification	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.	Preferred
7024	Data Security & Information Lifecycle Management Data Inventory / Flows	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.	Mandatory
7025	Data Security & Information Lifecycle Management eCommerce Transactions	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.	Preferred
7026	Data Security & Information Lifecycle Management Handling / Labeling / Security Policy	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.	Preferred
7027	Data Security & Information Lifecycle Management Non-Production Data	Production City data shall not be replicated or used in non-production environment without the expressed written of the City.	Mandatory
7028	Data Security & Information Lifecycle Management Ownership / Stewardship	All data shall be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	Preferred
7029	Data Security & Information Lifecycle Management Secure Disposal	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.	Mandatory

7030	Datacenter Security Asset Management	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.	Preferred
7031	Datacenter Security Controlled Access Points	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.	Mandatory
7032	Datacenter Security Equipment Identification	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.	Preferred
7033	Datacenter Security Off-Site Authorization	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.	Mandatory
7034	Datacenter Security Off-Site Equipment	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.	Preferred
7035	Datacenter Security Policy	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).	Preferred
7036	Datacenter Security - Secure Area Authorization	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.	Mandatory
7037	Datacenter Security Unauthorized Persons Entry	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.	Mandatory
7038	Datacenter Security User Access	Physical access to information assets and functions by users and support personnel shall be restricted.	Mandatory
7039	Encryption & Key Management Entitlement	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	Mandatory
7040	Encryption & Key Management Key Generation	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	Preferred

		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.	
7041	Encryption & Key Management Sensitive Data Protection	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.	Mandatory
7042	Encryption & Key Management Storage and Access	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.	Preferred
7043	Governance and Risk Management Baseline Requirements	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.	Preferred
7044	Governance and Risk Management Data Focus Risk Assessments	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	Preferred
7045	Governance and Risk Management Management Oversight	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.	Preferred

7046	Governance and Risk Management Management Program	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	Mandatory
7047	Governance and Risk Management Support/Involvement	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.	Preferred
7048	Governance and Risk Management Policy	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.	Preferred
7049	Governance and Risk Management Policy Enforcement	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.	Preferred
7050	Governance and Risk Management Policy Impact on Risk Assessments	Risk assessment results shall include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	Preferred
7051	Governance and Risk Management Policy Reviews	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.	Preferred

7052	Governance and Risk Management Risk Assessments	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).	Preferred
7053	Governance and Risk Management Risk Management Framework	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.	Mandatory
7054	Human Resources Asset Returns	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.	Preferred
7055	Human Resources Background Screening	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.	Preferred
7056	Human Resources Employment Agreements	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.	Preferred
7057	Human Resources Employment Termination	Roles and responsibilities for performing employment termination or change in employment procedures shall be assigned, documented, and communicated.	Preferred
7058	Human Resources Mobile Device Management	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).	Preferred
7059	Human Resources Non-Disclosure Agreements	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.	Mandatory

7060	Human Resources Roles / Responsibilities	Roles and responsibilities of contractors, employees, and third-party users shall be documented as they relate to information assets and security.	Mandatory
7061	Human Resources Technology Acceptable Use	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.	Preferred
7062	Human Resources Training / Awareness	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.	Preferred
7063	Human Resources User Responsibility	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	Preferred
7064	Human Resources Workspace	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.	Preferred
7065	Identity & Access Management Audit Tools Access	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.	Mandatory
7066	Identity & Access Management Credential Lifecycle / Provision Management	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	Preferred

		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, expirable, 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	
7067	Identity & Access Management Diagnostic / Configuration Ports Access	User access to diagnostic and configuration ports shall be restricted to authorized individuals and applications.	Preferred
7068	Identity & Access Management Policies and Procedures	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.	Preferred
7069	Identity & Access Management Segregation of Duties	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.	Preferred
7070	Identity & Access Management Source Code Access Restriction	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.	Preferred

7071	Identity & Access Management Third Party Access	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.	Mandatory
7072	Identity & Access Management Trusted Sources	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.	Preferred
7073	Identity & Access Management User Access Authorization	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.	Mandatory
7074	Identity & Access Management User Access Reviews	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.	Mandatory
7075	Identity & Access Management User Access Revocation	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.	Mandatory

7076	Identity & Access Management User ID Credentials	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, expirable, non-shared authentication secrets)	Preferred
7077	Identity & Access Management Utility Programs Access	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.	Mandatory
7078	Infrastructure & Virtualization Security Audit Logging / Intrusion Detection	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.	Mandatory
7079	Infrastructure & Virtualization Security Change Detection	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).	Mandatory
7080	Infrastructure & Virtualization Security Clock Synchronization	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.	Preferred
7081	Infrastructure & Virtualization Security Information System Documentation	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.	Preferred

7082	Infrastructure & Virtualization Security Management - Vulnerability Management	Implementers shall ensure that the security vulnerability assessment tools or services accommodate the virtualization technologies used (e.g. virtualization aware).	Mandatory
7083	Infrastructure & Virtualization Security Network Security	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.	Mandatory
7084	Infrastructure & Virtualization Security OS Hardening and Base Controls	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.	Mandatory
7085	Infrastructure & Virtualization Security Production / Non-Production Environments	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.	Mandatory
7086	Infrastructure & Virtualization Security Segmentation	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	Mandatory
7087	Infrastructure & Virtualization Security VM Security - vMotion Data Protection	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.	Mandatory
7088	Infrastructure & Virtualization Security	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	Mandatory

	VMM Security - Hypervisor Hardening	supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).	
7089	Infrastructure & Virtualization Security Wireless Security	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	Mandatory
7090	Infrastructure & Virtualization Security Network Architecture	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.	Mandatory
7091	Interoperability & Portability APIs	The provider shall use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	Preferred
7092	Interoperability & Portability Data Request	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)	Mandatory
7093	Interoperability & Portability Policy & Legal	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.	Preferred
7094	Interoperability & Portability Standardized Network Protocols	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.	Mandatory
7095	Interoperability & Portability Virtualization	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.	Preferred

7096	Mobile Security Anti-Malware	Anti-malware awareness training, specific to mobile devices, shall be included in the provider's information security awareness training.	Preferred
7097	Mobile Security Application Stores	A documented list of approved application stores has been defined as acceptable for mobile devices accessing or storing provider managed data.	Preferred
7098	Mobile Security Approved Applications	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.	Preferred
7099	Mobile Security Approved Software for BYOD	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.	Preferred
7100	Mobile Security Awareness and Training	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.	Preferred
7101	Mobile Security Cloud Based Services	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.	Mandatory
7102	Mobile Security Compatibility	The company shall have a documented application validation process to test for mobile device, operating system, and application compatibility issues.	Preferred
7103	Mobile Security Device Eligibility	The BYOD policy shall define the device and eligibility requirements to allow for BYOD usage.	Preferred
7104	Mobile Security Device Inventory	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.	Mandatory
7105	Mobile Security Device Management	A centralized, mobile device management solution shall be deployed to all mobile devices permitted to store, transmit, or process customer data.	Mandatory
7106	Mobile Security Encryption	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.	Preferred
7107	Mobile Security Jailbreaking and Rooting	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).	Preferred

7108	Mobile Security Legal	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.	Preferred
7109	Mobile Security Lockout Screen	BYOD and/or company-owned devices are configured to require an automatic lockout screen, and the requirement shall be enforced through technical controls.	Mandatory
7110	Mobile Security Operating Systems	Changes to mobile device operating systems, patch levels, and/or applications shall be managed through the company's change management processes.	Preferred
7111	Mobile Security Passwords	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.	Preferred
7112	Mobile Security Policy	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).	Preferred
7113	Mobile Security Remote Wipe	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.	Preferred
7114	Mobile Security Security Patches	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.	Mandatory
7115	Mobile Security Users	The BYOD policy shall clarify the systems and servers allowed for use or access on a BYOD-enabled device.	Preferred
7116	Security Incident Management, E-Discovery & Cloud Forensics Contact / Authority Maintenance	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.	Mandatory
7117	Security Incident Management, E-Discovery & Cloud Forensics Incident Management	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.	Preferred

7118	Security Incident Management, E-Discovery & Cloud Forensics Incident Reporting	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.	Mandatory
7119	Security Incident Management, E-Discovery & Cloud Forensics Incident Response Legal Preparation	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.	Mandatory
7120	Security Incident Management, E-Discovery & Cloud Forensics Incident Response Metrics	Mechanisms shall be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	Preferred
7121	Supply Chain Management, Transparency and Accountability Data Quality and Integrity	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.	Mandatory
7122	Supply Chain Management, Transparency and Accountability Incident Reporting	The provider shall make security incident information available to the City and providers periodically through electronic methods (e.g. portals).	Mandatory
7123	Supply Chain Management, Transparency and Accountability Network / Infrastructure Services	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.	Preferred

7124	Supply Chain Management, Transparency and Accountability Provider Internal Assessments	The provider shall perform annual internal assessments of conformance to, and effectiveness of, its policies, procedures, and supporting measures and metrics.	Mandatory
7125	Supply Chain Management, Transparency and Accountability Supply Chain Agreements	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	Preferred
7126	Supply Chain Management, Transparency and Accountability	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.	Preferred

	Supply Chain Governance Reviews		
7127	Supply Chain Management, Transparency and Accountability Supply Chain Metrics	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.	Preferred
7128	Supply Chain Management, Transparency and Accountability Third Party Assessment	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.	Mandatory
7129	Supply Chain Management, Transparency and Accountability Third Party Audits	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.	Preferred
7130	Threat and Vulnerability Management Anti-Virus / Malicious Software	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.	Preferred
7131	Threat and Vulnerability Management Vulnerability / Patch Management	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	Mandatory

		if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	
7132	Threat and Vulnerability Management Mobile Code	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.	Preferred

SCHEDULE B – DRAFT CONTRACT

CITY OF SURREY
the future lives here.

PROFESSIONAL SERVICES AGREEMENT

Title:	**Website, Virtual Exhibit – Being Punjabi**
Reference No.:	1220-030-2023-011

TABLE OF CONTENTS

[<⌨ insert page numbers]

Title: Website, Virtual Exhibit – Being Punjabi

THIS AGREEMENT is dated for reference this _____ day of _______________, 202_.

AGREEMENT No.: 1220-030-2023-011

BETWEEN:

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

(the "**City**")

AND:

____
(⌨ Insert Full Legal Name of Consultant)

(the "**Consultant**")

WHEREAS the City wishes to engage the Consultant to provide the Services and the Consultant agrees to provide the Services.

Website, Virtual Exhibit – Being Punjabi

THEREFORE, in consideration of the premises and 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 each party hereby acknowledges), the parties hereby covenant and agree with each other as follows:

1. INTERPRETATION

1.1 Definitions

In this agreement the following definitions apply:

"**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;

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

"**Disbursements**" has the meaning set out in Section 5.3;

"**Dispute**" has the meaning set out in Section 19.1;

"**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 5.1;

“**Indemnitees**” has the meaning set out in Section 7.1;

"**Invoice**" has the meaning set out in Section 5.2(a);

“**Services**” has the meaning set out in Section 2.1;

"**Term**" has the meaning set out in Section 2.5; and

“**Time Schedule**” has the meaning set out in Section 2.6.

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

1.2 Appendices

The following attached Appendices are a part of this agreement:

Appendix 1 – Scope of Services;
Appendix 1A – Functional and Technical Requirements;
Appendix 2 – Fees and Payment;
Appendix 3 – Time Schedule;
Appendix 4 – Personnel and Sub-Contractors;
Appendix 5 – Additional Services;
Appendix 6 – Privacy Protection Policy; and
Appendix 7 – Confidentiality Agreement.

2. SERVICES

2.1 Services

The City hereby retains the Consultant to provide the consulting and professional services as described generally in Appendix 1, including anything and everything required to be done for the fulfillment and completion of this agreement (the “**Services**”).

2.2 Amendment of Services

The City may from time to time, by written notice to the Consultant, make changes in the scope of the Services. The Fees will be increased or decreased by written agreement of the City and the Consultant according to the rates set out in Appendix 2.

2.3 Additional Services

The Consultant will, if requested in writing by the City, perform additional services as may be listed in Appendix 5. The terms of this agreement will apply to any additional services, and the fees for additional services, and the time for the Consultant’s performance, will generally correspond to the fees and time of performance as described in Appendices 2 and 3. The Consultant will not provide any additional services in excess of the scope of services requested in writing by the City.

2.4 Standard of Care

The Consultant 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 Consultant's experience and expertise. The Consultant represents that it has the expertise, qualifications, resources and relevant experience to provide the Services.

2.5 Term

The Consultant will provide the Services for the period commencing on June 1, 2023 and terminating on December 31, 2025 (the "**Term**").

The parties may extend the Term by mutual agreement. If the Term is extended, the provisions of this agreement will remain in force except where amended in writing by the parties.

2.6 Time

The Consultant acknowledges that time is of the essence with respect to the provision of the Services and accordingly the Consultant will provide the Services within the performance or completion dates or time periods (the "**Time Schedule**") as set out in Appendix 3, or as otherwise agreed to in writing by the City and the Consultant. If at any time the Consultant discovers that the Time Schedule cannot be met it will immediately advise the City in writing and provide a revised Time Schedule.

2.7 Optional Expansion of Services

(a) The City may, in its sole and absolute discretion, at any time after the first three (3) 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 determine at its election (a "Services Expansion"). The following will apply with respect to any Services Expansion:

  (1) 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

  (2) 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.

(b) 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 as described in this Agreement.

3. PERSONNEL AND SUB-CONTRACTORS

3.1 Qualified Personnel

The Consultant will provide only professional personnel who have the qualifications, experience and capabilities to perform the Services.

3.2 Listed Personnel and Sub-Contractors

The Consultant will perform the Services using the professional personnel and sub-contractors as may be listed in Appendix 4, and the Consultant will not remove any such listed personnel or sub-contractors from the Services without the prior written approval of the City.

3.3 Replacement of Personnel or Sub-Contractors

If the City reasonably objects to the performance, qualifications, experience or suitability of any of the Consultant’s personnel or sub-contractors then the Consultant will, on written request from the City, replace such personnel or sub-contractors.

3.4 Sub-Contractors and Assignment

Except as provided for in Section 3.2, the Consultant 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.

3.5 Agreements with Sub-Contractors

The Consultant 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 Consultant 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 Consultant.

4. LIMITED AUTHORITY

4.1 Agent of City

The Consultant is not and this agreement does not render the Consultant an agent or employee of the City, and without limiting the above, the Consultant 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 perform the Services. The Consultant will make such lack of authority clear to all persons with whom the Consultant deals in the course of providing the Services. Every vehicle used by the Consultant in the course of performing the services shall identify the Consultant by name and telephone number.

4.2 Independent Contractor

The Consultant 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 Consultant performs the Services. The Consultant will determine the number of days and hours of work required to properly and completely perform the

Services. The Consultant 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 Section 3.4. The Consultant will be solely liable for the wages, fringe benefits, work schedules and work conditions of any partners, employees or sub-contractors.

5. FEES

5.1 Fees

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

5.2 Payment

Subject to any contrary provisions set out in this Agreement:

(a) the Consultant will submit an invoice (the "**Invoice**") to the City requesting payment of the portion of the Fees and Disbursements relating to the Services provided. Each Invoice should be sent **electronically** to: surreyinvoices@surrey.ca and include the following information:

(1) an invoice number;
(2) the Consultant's name, address and telephone number;
(3) the City's reference number for the Services; P.O. # *(to be advised)*
(4) the names, charge-out rates and number of hours worked in the previous month of all employees of the Consultant and any sub-contractor(s) that has/have performed services during the previous month;
(5) the percentage of Services completed at the end of the previous month;
(6) the total budget for the Services and the amount of the budget expended to the date of the Invoice;
(7) taxes (if any);
(8) grand total of the Invoice;

(b) the Consultant will on request from the City provide receipts and invoices for all Disbursements claimed;

(c) if the City reasonably determines that any portion of an Invoice is not payable then the City will so advise the Consultant;

(d) the City will pay the portion of an Invoice which the City determines is payable less any deductions for setoffs or holdbacks permitted by this Agreement including, without limitation, any amounts permitted to be held back on account of deficiencies, within 30 days of the receipt of the Invoice;

(e) if the Consultant offers the City a cash discount for early payment, then the City may, at the City's sole discretion, pay the discounted portion of an Invoice; and

(f) all Invoices shall be stated in, and all payments made in, Canadian dollars.

5.3 Disbursements

In addition to the Fees, the City will reimburse the Consultant for actual out-of-pocket costs and expenses (“**Disbursements**”) as identified in Appendix 2 which the Consultant, and approved sub-contractors, incur in the performance of the Services, plus any additional Disbursements with the prior written approval of the City.

For greater certainty, costs of general management, non-technical supporting services and general overheads are deemed to be covered by the Fees and will not be subject to additional payment by the City.

5.4 Records

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

5.5 Non-Residents

If the Consultant 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 Consultant; or

(b) the amount required under applicable tax legislation.

6. CITY RESPONSIBILITIES

6.1 City Information

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

6.2 City Decisions

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

6.3 Notice of Defect

If the City observes or otherwise becomes aware of any fault or defect in the Services, it may notify the Consultant, but nothing in this agreement will be interpreted as giving the City the obligation to inspect or review the Consultant’s performance of the Services.

7. INSURANCE AND DAMAGES

7.1 Indemnity

The Consultant 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 Consultant of any obligation of this agreement, or any wrongful or negligent act or omission of the Consultant or any employee or agent of the Consultant.

7.2 Survival of Indemnity

The indemnity described in Section 7.1 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.

7.3 Consultant's Insurance Policies

The Consultant 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 ($3,000,000) dollars inclusive per occurrence against death, bodily injury and property damage arising directly or indirectly out of the work or operations of the Consultant, 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 Consultants protective liability, blanket contractual, employees as additional insureds, broad form property damage, non-owned automobile, contingent employers liability, broad form loss of use, personal injury, and incidental medical malpractice. The City will be added as additional insured;

(b) professional errors and omissions insurance in an amount not less two 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; and

(c) automobile liability insurance on all vehicles owned, operated or licensed in the name of the Consultant in an amount not less than three million ($3,000,000) dollars per occurrence for bodily injury, death and damage to property.

7.4 Insurance Requirements

The Consultant 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 Consultant will, on request from the City, provide certified copies of all of the Consultant’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 Consultant will be responsible for deductible amounts under the insurance policies. All of the Consultant's insurance policies will be primary and not require the sharing of any loss by the City or any insurer of the City.

7.5 Consultant Responsibilities

The Consultant 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 Consultant acknowledges and agrees that the Consultant 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 Consultant from responsibility for any amounts which may exceed these limits, for which the Consultant may be legally liable.

7.6 Additional Insurance

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

7.7 Waiver of Subrogation

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

8. TERMINATION

8.1 By the City

The City may at any time and for any reason by written notice to the Consultant terminate this agreement before the completion of all the Services, such notice to be determined by the City at its sole discretion. Upon receipt of such notice, the Consultant will perform no further Services other than the work which is reasonably required to terminate the Services and return the City’s property to the City. 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 Consultant all amounts owing under this agreement for Services provided by the Consultant 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 Consultant, 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.

8.2 Termination for Cause

The City may terminate this agreement for cause as follows:

(a) If the Consultant 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 Consultant or receiver or trustee in bankruptcy written notice; or

(b) If the Consultant 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 Consultant, then the City may, without prejudice to any other right or remedy the City may have, terminate this agreement by giving the Consultant further written notice.

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 Consultant 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 Consultant under this agreement, and at the completion of the Services pay to the Consultant any balance remaining; and

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

8.3 Curing Defaults

If the Consultant is in default of any of its obligations under this agreement, then the City may without terminating this agreement, upon 5 days written notice to the Consultant, remedy the default and set-off all costs and expenses of such remedy against any amounts owing to the Consultant. Nothing in this agreement will be interpreted or construed to mean that the City has any duty or obligation to remedy any default of the Consultant.

9. APPLICABLE LAWS, POLICIES, BUILDING CODES AND BY-LAWS

9.1 Applicable Laws and Policies

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

The Consultant shall comply with all applicable policies, procedures and instructions provided by the City.

9.2 Codes and By-Laws

The Consultant will provide the Services in full compliance with all applicable laws, building codes and regulations.

9.3 Interpretation of Codes

The Consultant will, as a qualified and experienced professional, interpret applicable codes, laws and regulations applicable to the performance of the Services. If an authority having jurisdiction imposes an interpretation which the Consultant 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.

10. CONFIDENTIALITY AND DISCLOSURE OF INFORMATION

10.1 No Disclosure

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

Refer to Attachment 2 – Confidentiality Agreement for additional information.

10.2 Freedom of Information and Protection of Privacy Act

The Consultant 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 Attachment 1 – Privacy Protection Schedule for additional information.

11. CITY DATA PRIVACY

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 City 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, the Contractor will not use such City Data for the Contractor's own benefit and, in particular, will not engage in “City 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 the City.

The Contractor will provide access to City Data only to those Contractor employees, agents, personnel, contractors and subcontractors who need to access the City Data to fulfill the Contractor's obligations under this Agreement. The Contractor will ensure that, prior to being granted access to the City Data, the Contractor's employees, agents or personnel 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 City Data protection provisions of this Agreement; and possess all qualifications appropriate to the nature of the Contractor's employees, agents and personnel's duties and the sensitivity of the City Data they will be handling.

The Contractor will ensure it maintains the confidentiality, integrity and availability of City Data by ensuring appropriate security controls are applied.

12. 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 service 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.

12.1 Access to City Data, Security Logs and Reports

The Contractor shall provide reports to the City in a format 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:

(a) 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

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

12.2 Import and Export of City Data

The City shall have the ability to import or export City 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 City Data to/from other service providers.

12.3 Access to and Extraction of City Data

The City shall have access to City's Data during the Term. The Contractor shall within seven (7) business days of the City's request, provide the City, without any contingencies whatsoever (including but not limited to payment of any fees due to the Contractor), an extract of the City 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 – Additional Work.

12.4 City Data Ownership

All City Data shall become and remain the property of the City. For greater certainty, when the Proponent makes changes to the source code, that changed source code will be considered City Data.

12.5 City Data Protection

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

(i) 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 the Contractor's own City Data of a similar type, and in no event less than reasonable in view of the type and nature of the City Data involved; and

(ii) 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.

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.

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.

12.6 City Data Destruction

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 City Data recovery is infeasible.

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

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

(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 of contractor.

13. SECURITY INCIDENT OR CITY DATA BREACH RESPONSE

13.1 When either a Security Incident or a City Data Breach is suspected, investigation is required to commence without delay. If the Contractor becomes aware of a suspected Security Incident or suspected City Data Breach, the Contractor will inform the City Clerk immediately (unless a City 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.

13.2 If a City 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.

13.3 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.

13.4 Oral reports by the Contractor regarding Security Incidents and City 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.

13.5 For any confirmed Security Incident, the Contractor's report discussed herein shall identify:

(a) the nature of the incident;
(b) the cause or suspected cause of the incident;
(c) what the Contractor has done or shall do to mitigate the incident; and

(d) what corrective action the Contractor has taken or shall take to prevent future similar incidents.

13.6 For an actual or suspected City Data Breach, the Contractor's report discussed herein shall identify:

(a) the nature of the unauthorized use or disclosure;
(b) the City Data used or disclosed;
(c) who made the unauthorized use or received the unauthorized disclosure (if known);
(d) what the Contractor has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure; and
(e) what corrective action the Contractor has taken or shall take to prevent future similar unauthorized use or disclosure.

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

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

13.9 Notwithstanding any other provision of this Agreement, and in addition to any other remedies available to the City under law or equity, the Contractor will promptly reimburse the City in full for all costs incurred by the City in any investigation, remediation or litigation resulting from any City Data Breach, including but not limited to providing notification to Third Parties whose City 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 City Data Breach in such a fashion that, in the 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 City Data Breach.

14. RETURN OF PROPERTY AND CITY DATA

The Contractor agrees to return to the City the City Data at the termination or expiration 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 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 SaaS. 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 herein.

15. INTELLECTUAL PROPERTY RIGHTS

15.1 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.

15.2 Neither party may transfer or assign it's rights and obligations under this agreement without first obtaining the other party's prior written consent.

16. USE OF WORK PRODUCT

The Consultant hereby sells, assigns and transfers to the City the right, title and interest required for the City to use and receive the benefit of all the reports, drawings, plans, designs, models, specifications, computer software, concepts, products, designs or processes or other such work product produced by or resulting from the Services rendered by the Consultant.

17. WORKERS' COMPENSATION BOARD AND OCCUPATIONAL HEALTH AND SAFETY

17.1 The Consultant agrees that it shall, at its own expense, procure and carry, or cause to be procured, carried and paid for, full Workers' Compensation Board coverage for itself and all workers, employees, servants and others engaged in or upon any work or service which is the subject of this agreement. The Consultant agrees that 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 owing by the City to the Consultant. 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 Services have been paid in full.

17.2 The Consultant will provide the City with the Consultant's Workers' Compensation Board registration number and a letter from the Workers' Compensation Board confirming that the Consultant is registered in good standing with the Workers' Compensation Board and that all assessments have been paid to the date thereof prior to the City having any obligations to pay monies under this agreement.

17.3 The Consultant agrees that it is the prime contractor for the Services as defined in the *Workers Compensation Act, R.S.B.C. 2019, c.1* as amended and will ensure compliance with the *Workers Compensation Act* and Regulations in respect of the workplace. Without limiting its responsibilities under the legislation, the Consultant will coordinate the activities of employers, workers and other persons at the workplace relating to occupational health and safety. The Consultant 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 Consultant 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 Consultant will advise the City immediately in writing if the name or contact number of the qualified coordinator changes.

17.4 Without limiting the generality of any other indemnities granted by the Consultant in this agreement, the Consultant shall indemnify and save harmless the Indemnitees from and against all claims, demands, causes of action, suits, losses, damages, costs, liabilities, expenses, judgements, 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.

17.5 The Consultant 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 Compensations Act* and Regulations pursuant thereto.

17.6 The City may, on twenty-four (24) hours written notice to the Consultant, 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 to ascertaining or discovering, through inspections or review of the operations of the Consultant or otherwise, any deficiency or immediate hazard.

18. BUSINESS LICENSE

18.1 The Consultant will obtain and maintain throughout the term of this agreement a valid City of Surrey business license.

19. DISPUTE RESOLUTION

19.1 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 19.

i. 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.

ii. <u>Mediation</u>

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.

iii. <u>Litigation</u>

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.

20. JURISDICTION AND COUNCIL NON-APPROPRIATION

20.1 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.

20.2 The Consultant 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 Consultant of its intention to terminate or reduce the services so affected within 30 days after the non-appropriation becomes final. Such termination shall take effect 30 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.

21. GENERAL

21.1 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.

21.2 Amendment

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

21.3 Consultant Terms Rejected

In the event that the Consultant 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.

21.4 Survival of Obligations

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

21.5 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.

21.6 Notices

Any notice, report or other document that either party may be required or may wish to give to the other should 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, five calendar days after posting. The addresses for delivery will be as follows:

(a) The City:

City of Surrey, Surrey City Hall
<⌨ insert department/division/section name>
13450 – 104th Avenue, Surrey, B.C., V3T 1V8, Canada

Attention: **<⌨ insert contact name>**
<⌨ insert title>

Business Fax No.: **<⌨ insert>**
Business Email: **<⌨ insert>**

(b) The Consultant (Contract Administrator):

<⌨ insert name and address>

Attention: **<⌨ insert contact name>**
<⌨ insert title>

Business Fax No.: **<⌨ insert>**
Business Email: **<⌨ insert>**

21.7 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.

21.8 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.

21.9 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.

21.10 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.

21.11 Signature

This agreement may be executed in 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.

21.12 Enurement

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

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

CITY OF SURREY

I/We have the authority to bind the City.

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

[⌨ INSERT FULL LEGAL NAME OF CONSULTANT]
I/We have the authority to bind the Consultant.

______________________________	______________________________
(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 7 WILL BE INSERTED LATER WHEN AN AGREEMENT IS ASSEMBLED FOR EXECUTION INCLUDING INFORMATION FROM THE RFP AND SUCCESSFUL PROPOSAL)

APPENDIX 1 – SCOPE OF SERVICES

APPENDIX 1A – FUNCTIONAL AND TECHNICAL REQUIREMENTS

APPENDIX 2 – FEES AND PAYMENT

APPENDIX 3 – TIME SCHEDULE

APPENDIX 4 – PERSONNEL AND SUB-CONTRACTORS

APPENDIX 5 – ADDITIONAL SERVICES

APPENDIX 6 – PRIVACY PROTECTION POLICY

APPENDIX 7 – CONFIDENTIALITY AGREEMENT

SCHEDULE C – FORM OF PROPOSAL

RFP Project Title: **Website, Virtual Exhibit - Being Punjabi**

RFP Reference No.: **1220-030-2023-011**

Legal Name of Proponent:

Contact Person and Title: ____

Business Address: ____

Business Telephone: ____

Business Fax: ____

Business E-Mail Address: ____

TO:
City Representative: Sunny Kaila, Manager, Procurement Services

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

Dear Sir:

1.0 I/We, the undersigned duly authorized representative of the Proponent, having received and carefully reviewed all of the Proposal documents, including the RFP and any issued addenda posted on the City Website and BC Bid Website, and having full knowledge of the Site, and having fully informed ourselves as to the intent, difficulties, facilities and local conditions attendant to performing the Services, submit this Proposal in response to the RFP.

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

Schedule C-1 – Statement of Departures;
Schedule C-2 – Proponent's Experience, Reputation and Resources;
Schedule C-3 – Proponent's Proposed Solution;
Schedule C-3-1 – Website, Virtual Exhibit - Being Punjabi Requirements Response;
Schedule C-4 – Proponent's Example Implementation Schedule; and
Schedule C-5 – Proponent's Financial Proposal:

3.0 **I/We confirm** that this Proposal 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 Solution. I/we further confirm that if I/we become aware that another consultant at the place(s) of the Solution 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 Proposal is submitted this ____day of ____________, 202_.

I/We have the authority to bind the Proponent.

____
(Legal Name of Proponent)

____ (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 RFP 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 Proponent 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 Consultant's Solution is subject to GST, the Consultant's GST Number is _____________________________________; and

(f) If the Consultant 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 Proposal, 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 RFP (list, if any):

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

____

____

4. The Proponent 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 - PROPONENT'S EXPERIENCE, REPUTATION AND RESOURCES

Proponents should provide information on the following (use the spaces provided and/or attach additional pages, if necessary

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

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

(iii) Proponent's demonstrated ability to provide the Services;

(iv) Proponent 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 RFP are as set out in Schedule A;

(v) Using a format similar to the following, provide a summary of similar relevant contracts entered into by the Proponent in which the Proponent 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 Proponent?	
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.	

(vi) Proponent's financial strength (with evidence such as financial statements, bank references);

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

(viii) Proponents should identify key personnel and their roles and responsibilities for all phases of the project. The Proponent should submit resumes and also a short narrative description of relevant experience for all proposed key personnel, for example:

- Account Manager
- Project Manager
- Design, Development and Implementation Manager
- Testing Manager
- Technical Architect

Name: ______________________________

Responsibility: ______________________________

Experience: ______________________________

____

(ix) Identify subcontractors, if any, the Proponent 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 - PROPONENT’S PROPOSED SOLUTION

Proponents should provide the following (use the spaces provided and/or attach additional pages, if necessary):

(i) **Letter of Introduction.** Provide an introduction to the Proponent, including a short description of the Proponent and their administrative team;

(ii) a narrative that illustrates an understanding of the City’s requirements and Services and describing the proposed solution;

(iii) a general description of the general approach and methodology that the Proponent would take in performing the Services including specifications and requirements;

(iv) provide in detail how Proponent’s proposed Solution meets the Website, Virtual Exhibit - Being Punjabi Requirements. Please complete **Website, Virtual Exhibit - Being Punjabi Requirements Response, Schedule C-3-1.**

Schedule C-3-1 may be viewed and/or downloaded from the City of Surrey’s Managed File Transfer Service (MFT):

Hostname:	https://mft.surrey.ca
Logon ID:	surreybid
Password:	Welcome

Locate Folder: 1220-030-2023-011

(v) **Value Added**: The Proponent should provide a description of value-added, innovative ideas and unique services that the Proponent can offer to implement the City’s requirements relevant to the scope of services described in this RFP; and

(vi) A description of the Proponents Information Security Management Program (ISMP) 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:

a. Risk management
b. Security policy
c. Organization of information security
d. Asset management
e. Human resources security
f. Physical and environmental security
g. Communications and operations management
h. Access control
i. Information systems acquisition, development, and maintenance

SCHEDULE C-4 - PROPONENT'S EXAMPLE IMPLEMENTATION SCHEDULE

Proponents should provide an estimated schedule, with major item descriptions and time indicating a commitment to perform the Contract within the time specified (use the spaces provided and/or attach additional pages, if necessary):

Proponent should indicate:

- Deliverable Work Product
- Service Start Date
- Work Product Delivery Date
- City Review Period (showing start and completion dates)

Deliverables	Service Start Date	Work Product Delivery Date	City Review Period	
			Start Date	Completed Date
	-	-	-	-

SCHEDULE C-5 - PROPONENT'S FINANCIAL PROPOSAL

1. Fee

Indicate the Proponent's proposed fee (excluding GST), using the following financial worksheet(s) (as applicable):

Phase	Description	Hours	Rate	Subtotal
1	Interpretive Plan - Content Grid - Architecture Diagram - List of Enhancements			
2	Preliminary Version - Prototype Website - Implement DMC changes			
3	Developed Version - Unilingual Website Version			
4	Final Version - Preliminary Landing Page - Fully Functional Website - Update Landing Page			
6	End User Training/Knowledge Transfer			
CURRENCY: Canadian **Note:** Overheads, General Conditions and Profit are to be included in the above amounts.			**Sub-Total:**	
			Taxes (5% GST):	
			Total:	

2. Additional Expenses:

The proposed Contract attached as Schedule "B" to the RFP 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:

3. 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.

ATTACHMENT 1 – PRIVACY PROTECTION SCHEDULE

(Included for reference purposes – will be attached to final agreement)

This Schedule forms part of the agreement between The City of Surrey (the "Public Body") and ___________ (the "Contractor") respecting Request for Proposals #1220-030-2023-011 – Website, Virtual Exhibit - Being Punjabi (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.

ATTACHMENT 2 – CONFIDENTIALITY AGREEMENT

This Schedule forms part of the agreement between City of Surrey (the "Public Body") and _______________ (the "Contractor") respecting Website, Virtual Exhibit - Being Punjabi, Request For Proposals #1220-030-2023-011 (the "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.

1. Primary Contact Person and Title: ______________________________

Business Address: ______________________________

Business Telephone: ______________________________

Business E-mail Address: ______________________________

____
(Signature of Authorized Signatory)

2. Secondary Contact Person and Title: ______________________________

Business Address: ______________________________

Business Telephone: ______________________________

Business E-mail Address: ______________________________

____
(Signature of Authorized Signatory)