REQUEST FOR PROPOSALS

Title: **City-Wide Wi-Fi Replacement**

Reference No.: 1220-030-2021-031

FOR PROFESSIONAL SERVICES (CONTRACTOR – GOODS AND SERVICES)

TABLE OF CONTENTS

REQUEST FOR PROPOSALS

1. INTRODUCTION

1.1 Purpose

Through this Request for Proposals (the "**RFP**"), the City of Surrey (the "**City**") is seeking proposals from proponents (each a "**Proponent**") to perform the services described in Schedule A – Scope of Services (the "**Services**"). That schedule, with such modifications as may be agreed between the City and the successful Proponent(s), will be incorporated into the contract between the City and the successful Proponent(s).

1.2 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;

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

"**Closing Time**" has the meaning set out in Section 2.1;

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

"**Evaluation Team**" means the team appointed by the City;

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

"**Information Meeting**" has the meaning set out in Section 2.2;

"**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 Goods are to be delivered and the Services are to be performed; and

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

2. INSTRUCTIONS TO PROPONENTS

2.1 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: **October 29, 2021**

(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.

2.2 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: **September 9, 2021**

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

Proponents interested in participating in this Information Meeting should email their requests to purchasing@surrey.ca

Time: **10:00 a.m. (PST)**

2.3 Site Visits

The City will be conducting site visits (the "Site Visits") as per Schedule A-2 – Site Visits. While attendance is at the discretion of Proponents, Proponents who do not attend will be deemed to have attended the Site Visits and to have received all of the information given at the Information Meeting.

2.4 Late Proposals

Proposals submitted after the Closing Time will not be accepted or considered. A Proponent bears all risk that the City's receiving computer equipment functions properly so that the Proposal is received by the Closing Time.

2.5 Amendments to Proposals

Proposals may be revised by written amendment, delivered to the location set out in Section 2.1, 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 3.2. 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 computer 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: Acting Manager, Procurement Services

E-mail: purchasing@surrey.ca

Reference: 1220-030-2021-031

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 and the City website at www.surrey.ca (collectively, the "**Websites**"), and upon posting, any addenda will form part of this RFP. It is the responsibility of Proponents to check the Websites 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 the Proponent is deemed to have received, accepted and understood the entire RFP, including any and all addenda.

2.8 Examination of Contract Documents and Site

Proponents will be deemed to have carefully examined the RFP, including all attached Schedules, the Contract and the Site (as applicable) prior to preparing and submitting a Proposal with respect to any and all facts which may influence a 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. PROPOSAL SUBMISSION FORM AND CONTENTS

3.1 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 Proponents are submitting Proposals in PDF format, it is preferred Proponents also submit their completed Schedule C-3-1 in Microsoft Excel.

3.2 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.

4. EVALUATION AND SELECTION

4.1 Evaluation Team

The evaluation of Proposals will be undertaken on behalf of the City by an evaluation team appointed by the City (the "**Evaluation Team**"), which may consist of one or more persons. 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.

4.2 Evaluation Criteria

The Evaluation Team will compare and evaluate all Proposals to determine each Proponent's strength and ability to provide the Services in order to determine the Proposal, or Proposals, which are most advantageous to the City, using the following criteria:

(a) Experience, Reputation and Resources – The Proponent's experience, reputation and resources as applicable to the performance of the Services.

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

(b) Technical – The Proponent's technical proposal for the performance of the Services as outlined in the Proponent's responses to items in Schedule C-3 and Schedule C-4.

(c) Financial – The Proponent's financial proposal for the performance of the Services as described in the Proponent's response to Schedule C-5.

(d) Statement of Departures - The Evaluation Team will consider the Proponent's response to Schedule C-1.

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. Specific weightings are not assigned to the individual evaluation criteria, but it is anticipated that the Proposal that offers the greatest overall value for money will be judged as most advantageous.

4.3 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;

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

4.4 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 contractors 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.

4.5 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.

4.6 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.

4.7 Multiple Preferred Proponents

The City reserves the right and discretion to divide up the Goods and 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 Goods and 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 Goods and Services and entering into one or more Contracts with one or more Proponents.

4.8 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) 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 Goods and 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 Goods and Services in some other manner.

5. GENERAL CONDITIONS

5.1 Reservation of Rights

Notwithstanding any other provision in this RFP, 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 right to at any time, and for any reason, reject all Proposals, and to terminate this RFP process without further explanation. The City is under no obligation to consider any Proposal, including the Proposal with the lowest price, or to select as the Preferred Proponent the Proponent that submits the Proposals with the lowest price.

5.2 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.

5.3 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.

5.4 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.

5.5 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 2.5, 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 seek an unfair advantage over other Proponents.

5.6 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.

5.7 No Claims

Each Proponent, by submitting a Proposal, irrevocably:

(a) agrees that it will not bring any claim, demand, action, cause of action, suit or proceeding, whether arising in contract, tort (including negligence) or otherwise (a "**Claim**") against the City or any of its employees, directors, officers, advisors or representatives, or any one of them, for any costs, damages or other compensation for any matter relating directly or indirectly to this RFP (including in the event that the City rejects or disqualifies or for any other reason fails to accept a Proposal, accepts a non-compliant Proposal or otherwise breaches, or fundamentally breaches, the terms of this RFP or any duties arising from this RFP; and

(b) waives any Claim against the City and its employees, directors, officers, advisors or representatives, or any one of them, for any compensation of whatsoever nature or kind, including for loss of anticipated profits, loss of opportunity, indirect, incidental or consequential damages or losses if no contract is entered into for the Services between the Proponent and the City for any reason whatsoever, including in the event that the City rejects or disqualifies or for any other reason fails to accept a Proposal, accepts a non-compliant Proposal or otherwise

breaches, or fundamentally breaches, the terms of this RFP or any duties arising from this RFP.

[End of Page]

SCHEDULE A – SPECIFICATIONS OF GOODS AND SCOPE OF SERVICES

1. Scope of Services

The City of Surrey (the "City") is inviting interested parties (hereafter referred to as "Proponent" or "Proponents") to present proposals for a solution to replace the City's current system which is reaching its end of life.

Proposals should include a centralized management and control system, access points, appropriate mounting brackets and hardware for all devices, VLAN integration, all necessary software, annual licensing, recurring costs, and on-site training and knowledge transfer for City network administrators. Proponents should note that the City is not interested in a managed solution.

The preference for this RFP is for new access points (APs) to provide similar coverage as is in place today. Ideally, new APs will simply replace old APs using the same mounting location and wiring. Many sites have AP placements imposed by in-building conduit and architecture which makes the relocation of an AP challenging. However, if the Proponent identifies a strong need to relocate APs or to upgrade wiring to assure satisfactory performance of the new Wi-Fi network, then provide details on what would be required.

Following is the description of the City's existing Wi-Fi infrastructure:

a) 114 SSIDs mapped to 99 unique VLANs/IP spaces
b) Open (public Wi-Fi), WPA2 (PSK), WP2 (802.1x certificate) authentication methods are currently used. Accommodation for future standards should be possible.
c) 44 VLAN/IP spaces used for Public Access, terminated to 3rd party data access controller for internet access services. Currently provided by Data Valet.
d) Dedicated 300Mbps internet circuit for Public Access is currently in place.
e) 2 VLAN/IP spaces used for telecom provider Wi-Fi integration. (Shaw Go Wi-Fi at City Hall and City Centre Library)
f) Remaining VLAN/IP spaces used for corporate issued mobile device access.
g) Typical WAP broadcasts 4-5 unique SSIDs, currently the maximum number of SSIDs on a single WAP is fourteen (14).
h) Four (4) Quality of Service (QoS) profiles to prioritize network traffic.
    (i) Priority queue for voice traffic (mainly Microsoft teams currently)
    (ii) Video (Mainly Microsoft Teams currently)
    (iii) Best effort
    (iv) Background
    (v) Local VLAN breakout

2. Security

Proponent will need to install and implement security features to ensure that proper security features are functioning with new and existing equipment. It will be of critical importance that our network is secure from unauthorized access both internally and externally. Design of the solution should comply with generally accepted security best practises.

3. RCMP Security Clearance

The awarded Proponent will be required to obtain RCMP Security Clearance. Proponents should be prepared to apply for security clearance immediately upon award so that work can be commenced immediately.

4. Training & Documentation

The implementation of the wireless network should include operational training and hand off to City staff when the implementation is complete. Detailed documentation for all aspects of installed network including high level and detailed design documentation, heat charts, network diagrams and technical/configuration notes/explanations will be required. All Proposals should indicate the training areas covered.

5. Support

Proponent will coordinate with vendors to provide warranty support for all hardware and software for the duration of the implementation. Proponent should outline, in detail, the service and support options that are available to the City.

6. Optional Sites

The Proponent may also provide separate solution pricing for the following sites:

6.1. Holland Park outdoor coverage

6.1.1. Single Wireless Controller
6.1.2. 10 Outdoor mesh access points located in a park.
6.1.3. 1 Wireless LANs mapped to 1 unique VLANs/IP space for Public Access.
6.1.4. Used during outdoor events/festivals.
6.1.5. 110V power adapters

6.2. Additional/New Considerations

6.2.1. Outdoor access points to cover outdoor locations.
6.2.1.1. Bill Reid Millennium Amphitheatre
6.2.1.2. Newton Athletics Park (grandstand and park areas)
6.2.1.3. South Surrey Athletic Park

SCHEDULE A-1 – CITY-WIDE WI-FI REPLACEMENT

For greater certainty, the requirements listed in Schedule A-1 – City-Wide Wi-Fi Replacement and Schedule C-3-1 – City-Wide Wi-Fi Replacement 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.

Requirements numbered 3### (3000's), 4### (4000's) and 5### (5000's) are only applicable if the Proponent is Proposing a solution that includes a web application, mobile application, and/or cloud service.

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	surreybid
Password:	Welcome
Locate Folder	1220-030-2021-031

[END OF PAGE]

FUNCTIONAL REQUIREMENTS

Req. #	Requirement	Level of Need
SOLUTION SPECIFICATIONS		
1000	Include at least 400 access points distributed across 50+ locations (List of locations is included.) - 25 large campus locations connected by high-speed managed fibre services. A large location will have more than 5 access points. - Remaining small locations connected by VPN over consumer internet. A small location will have less than 5 access points.	Mandatory
1001	Include indoor directional, high-capacity access points for grandstand coverage in all Ice Arena locations.	Preferred
1002	WAPs must support VLAN tagging on individual SSID's.	Mandatory
1003	WAPs must have the ability to switch radios (programmable) from the 2.4 GHz spectrum to the 5 GHz spectrum.	Mandatory
1004	Proposed network equipment should be upgradeable to support industry standards. Proponent is required to provide a written description of upgradeability and how their proposal addresses this specification relative to industry standards	Preferred
1005	Proposed Network solution should provide industry standard wireless encryption performed at the access point	Preferred
1006	The Network Wi-Fi controller should allow for scalability for future expansion.	Preferred
1007	Wireless Access Points (WAP) can be a blend of indoor (built in antennas) and or outdoor (external antennas).	Preferred
1008	WAPs should include a built-in spectrum analyzer.	Preferred
1009	The Wi-Fi infrastructure should have enough capacity to support a minimum of 2500 simultaneous Wi-Fi users. - Approximately 1500 Public mobile devices - Approximately 1000 corporate issued mobile devices.	Preferred
1010	Proponent should describe options for redundancy of proposed implementation at the WAP, Radio, Uplink, Backhaul and Power-Supply level and itemize what is included in their Proposal.	Preferred
1011	Reuse of existing WAP locations and network wiring is preferred to minimize site disruption. If the Proponent determines that their proposed solution requires changes to the current WAP locations and/or network wiring, they should include those changes in their proposed solution.	Preferred
1012	All integration/management software should be compatible with current Windows operating systems.	Preferred
1013	All WAPs should fully support Windows, OS X, iOS, and Android devices including, but not limited to laptops, tablets, smartphones, printers, and other wireless capable devices.	Preferred

DESIGN AND IMPLEMENTATION		
1014	Design and work with the City to implement the new Wi-Fi network.	Mandatory
1015	Procure/implement all hardware/software needed to accomplish this project.	Mandatory
1016	Procure licensing/implement all required software to accomplish this project. Including centralized management and control system.	Mandatory
1017	Provide any required networking services to implement your proposed design.	Mandatory
1018	Work with the City to configure the new Wi-Fi to work in conjunction with existing content filtering and firewall appliance.	Mandatory
1019	Provide on-site training for the new wireless network to the City IT staff.	Mandatory
1020	Implement best security practices across all sites utilizing proposed/existing hardware/software to prevent unauthorized access.	Mandatory
1021	Ensure any new cables running to access points conform to relevant building codes.	Mandatory
1022	Once the implementation of the new network is completed, provide a final quality control check to ensure all required elements are complete, accurate, and adaptable to the specifications contemplated in this Scope. All work not found in conformance with the intent of the Proposal shall be repaired promptly at no additional charge.	Mandatory
1023	Provide technical support (either onsite or remotely) at no additional cost, for problems that occur due to design/implementation issues for a period of 60 days after the completion date of this project.	Mandatory
1024	The City has experience with, and is comfortable using, “on-premises” hardware controllers. However, the City is not opposed to using virtual controllers or a cloud managed system provided it can meet the same performance, security, reliability, and availability metrics. If a cloud managed solution is proposed, it must conform to the City’s data residency requirements that no City data be stored outside of Canada. Contact the City if you want a copy of the policy.	Mandatory
TRAINING AND SUPPORT		
1025	Include operational training and hand off to City staff when the implementation is complete. Detailed documentation for all aspects of installed network including high level and detailed design documentation, heat charts, network diagrams and technical/configuration notes/explanations will be required. All Proposals should indicate the training areas covered.	Preferred

OTHER CONSIDERATIONS		
1026	Provide separate solutioning and pricing for the following: • Holland Park outdoor coverage that includes: - Single Wireless Controller - 10 Outdoor mesh access points located in a park. - 1 Wireless LANs mapped to 1 unique VLANs/IP space for Public Access. - Used during outdoor events/festivals. - 110V power adapters	Desired
1027	Additional/New Considerations • Outdoor access points to cover outdoor locations: - Cloverdale Bill Reid Millennium Amphitheatre - Newton Athletics Park (grandstand and park areas) - South Surrey Athletic Park, Bear Creek Park	Desired

GENERAL SECURITY REQUIREMENTS

Access Control (Wi-Fi System Administration)			
Req. #	**Category**	**Requirement**	**Level of Need**
2000	User Authentication / Secure Login	System access must be controlled by a secure login procedure the authenticates a user's identity.	Mandatory
2001	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
2002	Roles Based Access / Authorization	The system must support roles based (or group based) access control.	Mandatory

2003	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
2004	Multi-Factor Authentication (MFA)	The system should support the use of the City's Multi-Factor authentication solution (AZURE AD MFA) for access from untrusted locations.	Preferred
2005	User Access Provisioning	The system should support automatic user provisioning/de-provisioning. Note: This requirement can be ignored if AD integration is possible.	Preferred
2006	Privileged Account Management	The system should support integration with leading Privileged Identity Management solutions.	Desired
2007	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**
2008	Encryption of Data in Transit	The system must support the encryption of City data while in transit.	Mandatory
2009	Encryption of Data at Rest	The system must support the encryption of City data while at rest.	Mandatory if Cloud, otherwise Preferred
2010	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**
2011	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

2012	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.	Mandatory
2013	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**
2014	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
2015	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
3000	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, password strength best practice).	Preferred
3001	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
3002	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

3003	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
3004	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
3005	Web Error Handling and Logging	All web applications should fail securely, and not reveal any sensitive or application configuration information in error messages.	Preferred
3006	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
3007	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
3008	API Security	API security should be key, secret and time-limited token based. If not, then please specify API security strategy.	Preferred

MOBILE APP SECURITY REQUIREMENTS

Req. #	Category	Requirement	Level of Need
4000	Data Protection	Any sensitive data (PII, Credit Card Data, Financial and other sensitive City data) cached or stored on a mobile device must be encrypted by the mobile application. Ideally, AES 256-bit encryption is used, however, 128-bit AES or algorithms of similar (or greater) strength is sufficient. In addition, CoS must have the ability to configure a data deletion purge age (delete of X amount of time), and remotely wipe any corporate data on corporate or personal devices (corporate applications). Transmission of any sensitive data between the mobile application and a backend server must be encrypted using TLS 1.2 or higher. Corporate applications should leverage mutual authentication as part of the encryption process (server and client certs required for nailing up a TLS session).	Mandatory

4001	Mobile Access Control	Mobile applications accessing, collecting, processing, or storing sensitive data (PII, Credit Card Data, Financial and other sensitive City data) information must uniquely identify users and secure access with a strong password (8 character minimum). These passwords should not be stored on the device in any format, (even if hashed or encrypted; however, the risk is significantly less if passwords are encrypted or hashed) or viewable in any application cache or log file. Corporate application must comply with the existing password policy, and must provide support for Multifactor Authentication (MFA) for granting access (certificate, biometric, etc.). Proponent can ask for City's password policies if desired.	Mandatory
4002	Mobile Vulnerability Management	Mobile applications should be regularly tested for vulnerabilities, either by the vendor or an internal city team. Patches should be applied as soon as they are available from the vendor and tested. Anti-malware support should be provided when needed (apps designed to run on Android and Windows platforms).	Preferred

CLOUD SECURITY REQUIREMENTS

Req. #	Category	Requirement	Level of Need
5000	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
5001	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
5002	Application & Interface Security Data Integrity	Data input and output integrity routines (i.e., reconciliation and edit checks) should be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	Preferred
5003	Application & Interface Security Data Security / Integrity	Policies and procedures should 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

5004	Audit Assurance & Compliance Audit Planning	Audit plans should 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
5005	Audit Assurance & Compliance Independent Audits	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	Mandatory
5006	Audit Assurance & Compliance Information System Regulatory Mapping	Organizations should create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework - should be reviewed at least annually to ensure changes that could affect the business processes are reflected.	Preferred
5007	Business Continuity Management & Operational Resilience Business Continuity Planning	A consistent unified framework for business continuity planning and plan development should 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
5008	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

5009	Business Continuity Management & Operational Resilience Datacenter Utilities / Environmental Conditions	Datacentre utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) should 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
5010	Business Continuity Management & Operational Resilience Documentation	Information system documentation (e.g., administrator and user guides, and architecture diagrams) should 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
5011	Business Continuity Management & Operational Resilience Environmental Risks	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.	Mandatory
5012	Business Continuity Management & Operational Resilience Equipment Location	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment should be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.	Preferred
5013	Business Continuity Management & Operational Resilience Equipment Maintenance	Policies and procedures should be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.	Preferred
5014	Business Continuity Management & Operational Resilience Equipment Power Failures	Protection measures should be put into place to react to natural and man-made threats based upon a geographically specific Business Impact Assessment	Preferred

5015	Business Continuity Management & Operational Resilience Impact Analysis	There should 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
5016	Business Continuity Management & Operational Resilience Policy	Policies and procedures should be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures should include defined roles and responsibilities supported by regular workforce training.	Preferred
5017	Business Continuity Management & Operational Resilience Retention Policy	Policies and procedures should 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 should be incorporated as part of business continuity planning and tested accordingly for effectiveness.	Preferred
5018	Change Control & Configuration Management New Development / Acquisition	Policies and procedures should 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

5019	Change Control & Configuration Management Outsourced Development	External business partners should 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
5020	Change Control & Configuration Management Quality Testing	Organization should 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
5021	Change Control & Configuration Management Unauthorized Software Installations	Policies and procedures should 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
5022	Change Control & Configuration Management Production Changes	Policies and procedures should be established for managing the risks associated with applying changes to: • business-critical or customer (tenant)-impacting (physical and virtual) applications and system-system interface (API) designs and configurations • infrastructure network and systems components Technical measures should 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.	Preferred
5023	Data Security & Information Lifecycle Management Classification	Data and objects containing data should be assigned a classification by the data owner based on data type, value, sensitivity, and criticality to the organization.	Preferred
5024	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

5025	Data Security & Information Lifecycle Management eCommerce Transactions	Data related to electronic commerce (e-commerce) that traverses public networks should 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
5026	Data Security & Information Lifecycle Management Handling / Labeling / Security Policy	Policies and procedures should be established for the labeling, handling, and security of data and objects which contain data. Mechanisms for label inheritance should be implemented for objects that act as aggregate containers for data.	Preferred
5027	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
5028	Data Security & Information Lifecycle Management Ownership / Stewardship	All data should be designated with stewardship, with assigned responsibilities defined, documented, and communicated.	Preferred
5029	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
5030	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 should be maintained and updated regularly and assigned ownership by defined roles and responsibilities.	Preferred
5031	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
5032	Datacenter Security Equipment Identification	Automated equipment identification should 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

5033	Datacenter Security Off-Site Authorization	Authorization must be obtained prior to relocation or transfer of hardware, software, or data to an offsite premises.	Mandatory
5034	Datacenter Security Off-Site Equipment	Policies and procedures should be established for the secure disposal of computing equipment. This should include a wiping solution or destruction process that renders recovery of information impossible. The erasure should 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
5035	Datacenter Security Policy	Policies and procedures should 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
5036	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
5037	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
5038	Datacenter Security User Access	Physical access to information assets and functions by users and support personnel shall be restricted.	Mandatory
5039	Encryption & Key Management Entitlement	Keys must have identifiable owners (binding keys to identities) and there shall be key management policies.	Mandatory
5040	Encryption & Key Management Key Generation	Policies and procedures should be established for the management of cryptographic keys in the service's cryptosystem (e.g., lifecycle management from key generation to revocation and replacement, public key infrastructure, cryptographic protocol design and algorithms used, access controls in place for secure key generation, and exchange and storage including segregation of keys used for encrypted data or sessions). Upon request, provider should 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.	Preferred

5041	Encryption & Key Management Sensitive Data Protection	Policies and procedures must 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
5042	Encryption & Key Management Storage and Access	Platform and data-appropriate encryption (e.g., AES-256) in open/validated formats and standard algorithms should be required. Keys should 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 should be separated duties.	Preferred
5043	Governance and Risk Management Baseline Requirements	Baseline security requirements should 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
5044	Governance and Risk Management Data Focus Risk Assessments	Risk assessments associated with data governance requirements should be conducted at planned intervals and should 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
5045	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

5046	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
5047	Governance and Risk Management Management Support/Involvement	Executive and line management should take formal action to support information security through clearly documented direction, commitment and ensure the action has been assigned.	Preferred
5048	Governance and Risk Management Policy	Information security policies and procedures should 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
5049	Governance and Risk Management Policy Enforcement	A formal disciplinary or sanction policy should be established for employees who have violated security policies and procedures. Employees should 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
5050	Governance and Risk Management Policy Impact on Risk Assessments	Risk assessment results should include updates to security policies, procedures, standards, and controls to ensure that they remain relevant and effective.	Preferred

5051	Governance and Risk Management Policy Reviews	The organization's business leadership (or other accountable business role or function) should review the information security policy at planned intervals or because 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
5052	Governance and Risk Management Risk Assessments	Aligned with the enterprise-wide framework, formal risk assessments should 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 should be determined independently, considering all risk categories (e.g., audit results, threat and vulnerability analysis, and regulatory compliance).	Preferred
5053	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
5054	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) should be returned within an established period.	Preferred
5055	Human Resources Background Screening	Pursuant to local laws, regulations, ethics, and contractual constraints, all employment candidates, contractors, and third parties should be subject to background verification proportional to the data classification to be accessed, the business requirements, and acceptable risk.	Preferred
5056	Human Resources Employment Agreements	Employment agreements should 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
5057	Human Resources Employment Termination	Roles and responsibilities for performing employment termination or change in employment procedures should be assigned, documented, and communicated.	Preferred

5058	Human Resources Mobile Device Management	Policies and procedures should 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
5059	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
5060	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
5061	Human Resources Technology Acceptable Use	Policies and procedures should 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) should be considered and incorporated as appropriate.	Preferred
5062	Human Resources Training / Awareness	A security awareness training program should be established for all contractors, third-party users, and employees of the organization and mandated when appropriate. All individuals with access to organizational data should receive appropriate awareness training and regular updates in organizational procedures, processes, and policies relating to their professional function relative to the organization.	Preferred
5063	Human Resources User Responsibility	All personnel should 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
5064	Human Resources Workspace	Policies and procedures should 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

5065	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
5066	Identity & Access Management Credential Lifecycle / Provision Management	User access policies and procedures should be established, and supporting business processes and technical measures implemented, for ensuring appropriate identity, entitlement, and access management for all internal corporate and customer (tenant) users with access to data and organizationally owned or managed (physical and virtual) application interfaces and infrastructure network and systems components. These policies, procedures, processes, and measures should incorporate the following: • Procedures and supporting roles and responsibilities for provisioning and de-provisioning user account entitlements following the rule of least privilege based on job function (e.g., internal employee and contingent staff personnel changes, customer-controlled access, suppliers' business relationships, or other third-party business relationships) • Business case considerations for higher levels of assurance and multi-factor authentication secrets (e.g., management interfaces, key generation, remote access, segregation of duties, emergency access, large-scale provisioning or geographically-distributed deployments, and personnel redundancy for critical systems) • Access segmentation to sessions and data in multi-tenant architectures by any third party (e.g., provider and/or other customer (tenant)) • Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and federation) • Account credential lifecycle management from instantiation through revocation • Account credential and/or identity store minimization or re-use when feasible • Authentication, authorization, and accounting (AAA) rules for access to data and sessions (e.g., encryption and strong/multi-factor, 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	Preferred

5067	Identity & Access Management Diagnostic / Configuration Ports Access	User access to diagnostic and configuration ports should be restricted to authorized individuals and applications.	Preferred
5068	Identity & Access Management Policies and Procedures	Policies and procedures should be established to store and manage identity information about every person who accesses IT infrastructure and to determine their level of access. Policies should also be developed to control access to network resources based on user identity.	Preferred
5069	Identity & Access Management Segregation of Duties	User access policies and procedures should 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
5070	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 should be appropriately restricted following the rule of least privilege based on job function as per established user access policies and procedures.	Preferred
5071	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
5072	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

5073	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
5074	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
5075	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

5076	Identity & Access Management User ID Credentials	Internal corporate or customer (tenant) user account credentials should 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
5077	Identity & Access Management Utility Programs Access	Utility programs capable of potentially overriding system, object, network, virtual machine, and application controls shall be restricted.	Mandatory
5078	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
5079	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
5080	Infrastructure & Virtualization Security Clock Synchronization	A reliable and mutually agreed upon external time source should be used to synchronize the system clocks of all relevant information processing systems to facilitate tracing and reconstitution of activity timelines.	Preferred

5081	Infrastructure & Virtualization Security Information System Documentation	The availability, quality, and adequate capacity and resources should 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 should be made to mitigate the risk of system overload.	Preferred
5082	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
5083	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
5084	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
5085	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

5086	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
5087	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
5088	Infrastructure & Virtualization Security VMM Security - Hypervisor Hardening	Access to all hypervisor management functions or administrative consoles for systems hosting virtualized systems shall be restricted to personnel based upon the principle of least privilege and supported through technical controls (e.g., two-factor authentication, audit trails, IP address filtering, firewalls, and TLS encapsulated communications to the administrative consoles).	Mandatory
5089	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

5090	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
5091	Interoperability & Portability APIs	The provider should use open and published APIs to ensure support for interoperability between components and to facilitate migrating applications.	Preferred
5092	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
5093	Interoperability & Portability Policy & Legal	Policies, procedures, and mutually agreed upon provisions and/or terms should 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
5094	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
5095	Interoperability & Portability Virtualization	The provider should use an industry-recognized virtualization platform and standard virtualization formats (e.g., OVF) to help ensure interoperability, and should have documented custom changes made to any hypervisor in use and all solution-specific virtualization hooks available for customer review.	Preferred
5096	Mobile Security Anti-Malware	Anti-malware awareness training, specific to mobile devices, should be included in the provider's information security awareness training.	Preferred
5097	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
5098	Mobile Security Approved Applications	The company should have a documented policy prohibiting the installation of non-approved applications or approved applications not obtained through a pre-identified application store.	Preferred

5099	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
5100	Mobile Security Awareness and Training	The provider should 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 should post and communicate the policy and requirements through the company's security awareness and training program.	Preferred
5101	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
5102	Mobile Security Compatibility	The company should have a documented application validation process to test for mobile device, operating system, and application compatibility issues.	Preferred
5103	Mobile Security Device Eligibility	The BYOD policy should define the device and eligibility requirements to allow for BYOD usage.	Preferred
5104	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
5105	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
5106	Mobile Security Encryption	The mobile device policy should require the use of encryption either for the entire device or for data identified as sensitive on all mobile devices and should be enforced through technology controls.	Preferred
5107	Mobile Security Jailbreaking and Rooting	The mobile device policy should prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting) and should enforce the prohibition through detective and preventative controls on the device or through a centralized device management system (e.g., mobile device management).	Preferred
5108	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 should clearly state the expectations regarding the loss of non-company data in the case a wipe of the device is required.	Preferred
5109	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

5110	Mobile Security Operating Systems	Changes to mobile device operating systems, patch levels, and/or applications should be managed through the company's change management processes.	Preferred
5111	Mobile Security Passwords	Password policies, applicable to mobile devices, should be documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and should prohibit the changing of password/PIN lengths and authentication requirements.	Preferred
5112	Mobile Security Policy	The mobile device policy should 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
5113	Mobile Security Remote Wipe	All mobile devices permitted for use through the company BYOD program, or a company-assigned mobile devices should allow for remote wipe by the company's corporate IT or should have all company-provided data wiped by the company's corporate IT.	Preferred
5114	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
5115	Mobile Security Users	The BYOD policy should clarify the systems and servers allowed for use or access on a BYOD-enabled device.	Preferred
5116	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
5117	Security Incident Management, E-Discovery & Cloud Forensics Incident Management	Policies and procedures should 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

5118	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
5119	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
5120	Security Incident Management, E-Discovery & Cloud Forensics Incident Response Metrics	Mechanisms should be put in place to monitor and quantify the types, volumes, and costs of information security incidents.	Preferred
5121	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
5122	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

5123	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, should 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
5124	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

5125	Supply Chain Management, Transparency and Accountability Supply Chain Agreements	Supply chain agreements (e.g., SLAs) between providers and customers (tenants) should 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
5126	Supply Chain Management, Transparency and Accountability Supply Chain Governance Reviews	Providers should 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

5127	Supply Chain Management, Transparency and Accountability Supply Chain Metrics	Policies and procedures should 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 should be 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
5128	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
5129	Supply Chain Management, Transparency and Accountability Third Party Audits	Third-party service providers should 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 should undergo audit and review at least annually to govern and maintain compliance with the service delivery agreements.	Preferred
5130	Threat and Vulnerability Management Anti-Virus / Malicious Software	Policies and procedures should 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

5131	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 if customer (tenant) data is used as part the service and/or customer (tenant) has some shared responsibility over implementation of control.	Mandatory
5132	Threat and Vulnerability Management Mobile Code	Policies and procedures should 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 A-2 – SITE VISITS

Site Visits will be conducted as per the schedule below.

The expected duration of each site visit is an approximation of duration only. Approximately 20 minutes of travel time will be allotted between sites.

[End of Page]

Site	Address	Date	Expected Duration (Hours)	Notes
North				
City Hall, City Centre Library, & 3 Civic Plaza	13450 104 Avenue	September 20, 2021	2.5	Meet in lobby of City Hall.
North Surrey Sports & Ice Complex	10950 126A Street	September 20, 2021	1.0	
RCMP - Whalley/City Centre District Office 1	10720 King George Boulevard	September 20, 2021	1.0	
Chuck Bailey Recreation	13458 107A Avenue	September 21, 2021	1.0	Meet inside main entrance.
Bridgeview Community Centre	11475 126A Street	September 21, 2021	1.0	
West Village Boiler Plant	13231 Central Avenue	September 21, 2021	1.0	
RCMP - Guildford District Office 2	10395 148 Street	September 22, 2021	1.0	Meet inside main entrance.
Guildford Campus - Library/Recreation/Aquatics	15105 105 Avenue	September 22, 2021	2.5	Meet in upper lobby area near Library entrance.
Hemlock Operations	9353 160 Street	September 22, 2021	1.0	
Fraser Heights Recreation	10588 160 Street	September 22, 2021	1.0	
Central East				
Animal Center	17944 Colebrook Road	September 23, 2021	1.5	Meet inside main entrance.
Cloverdale Museum & Campus - Archives & Library	17710 56 Avenue	September 23, 2021	1.5	Meet at Musuem to start the tour
RCMP - Cloverdale District Office 4	5732 176A Street	September 23, 2021	1.0	
Cloverdale Recreation & Arena	6188 176 Street	September 23, 2021	1.5	Meet at Recreation Center start tour
Port Kells Library	18885 88 Avenue	September 23, 2021	1.5	
Clayton Community Center	7155 187A Street	September 23, 2021	1.0	
Clayton Hall	18513 70 Avenue	September 23, 2021	0.5	
Central West				
Fire Hall 1	8767 132 Street	September 24, 2021	1.5	Meet in parking lot near main entrance.
Surrey Fire Training Centre	1491 64 Avenue	September 24, 2021	1.5	Meet at STFC building start tour
Operation Centre Administration & Fleet Buildings	6651 148 Street	September 24, 2021	1.5	
Arts Centre	13750 88 Avenue	September 27, 2021	1.5	Meet inside main entrance.
RCMP - Newton District Office 3	7235 137 Street	September 27, 2021	1.0	
Newton Campus - Pools/Arena/Seniors/Library	13730 72 Avenue	September 27, 2021	1.5	Meet at Wave Pool to start tour.
Strawberry Hill Library	7399 122 Street	September 27, 2021	1.5	
Old City Hall - North Annex, RCMP, & West Wing	14355 57 Avenue	September 27, 2021	1.5	
South				
Darts Hill	1660 168 Street	September 28, 2021	1.0	Meet at car park.
Grandview Heights Aquatics Centre	16855 24 Avenue	September 28, 2021	1.0	
South Surrey Operations Centre	16666 24 Avenue	September 28, 2021	1.0	
Semiahmoo Library	200-1815 152 Street	September 28, 2021	1.0	
Surrey Cemetery	14850 28 Avenue	September 29, 2021	1.0	Meet at car park.
South Surrey Pool - Recreation & Arena	14655 17 Avenue	September 29, 2021	1.0	Start at pool to start tour
RCMP - South Surrey District Office 5	#100-1815 152 Street	September 29, 2021	1.0	
Ocean Park Library	12854 17 Avenue	September 29, 2021	1.0	

Optional Sites				
Site	**Address**	**Date**	**Expected Duration**	**Notes**
Holland Park - Outdoor Coverage	13428 Old Yale Road	September 30, 2021	1.0	
Bill Reid Millennium Amphitheatre	17728 64 Avenue	September 30, 2021	1.0	
Newton Athletics Park (Grandstand & Park Areas)	7395 128 Street	September 30, 2021	1.0	
South Surrey Athletic Park	14600 20 Avenue	September 30, 2021	1.0	

[End of Page]

SCHEDULE B – DRAFT CONTRACT

PROFESSIONAL SERVICES AGREEMENT

Title: **City-Wide Wi-Fi Replacement**

Reference No.: 1220-030-2021-031

TABLE OF CONTENTS

Title: City-Wide Wi-Fi Replacement

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

AGREEMENT No.: 1220-030-2021-031

BETWEEN:

CITY OF SURREY
13450 - 104 Avenue
Surrey, B.C., V3T 1V8, Canada

(the "**City**")

AND:

_____
(Insert Full Legal Name and Address of Contractor)

(the "**Contractor**")

WHEREAS the City wishes to engage the Contractor to provide the Goods and Services and the Contractor agrees to provide the Goods and Services.

City-Wide Wi-Fi Replacement

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:

"**Dispute**" has the meaning set out in Section 14.1;

"**Fees**" has the meaning set out in Section 5.1;

"**Goods**" has the meaning set out in Section 2.1;

"**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.

1.2 Appendices

The following attached Appendices are a part of this agreement:

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

2. GOODS AND SERVICES

2.1 Goods and Services

The City hereby retains the Contractor to provide the Goods and Services as described generally in Appendix 1, including anything and everything required to be done for the fulfillment and completion of this agreement (the "**Goods and Services**").

2.2 Amendment of Goods and Services

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

2.3 Additional Goods and Services

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

2.4 Standard of Care

The Contractor will provide the Goods and perform the Services with that degree of care, skill and diligence normally provided by a qualified and experienced practitioner. The Contractor represents that it has the expertise, qualifications, resources and relevant experience to provide the Goods and Services.

2.5 Term

The Contractor will provide the Goods and Services for the period commencing on (START DATE) and terminating on (END DATE) (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 Contractor acknowledges that time is of the essence with respect to the provision of the Goods and Services and accordingly the Contractor will provide the Goods and 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 Contractor. If at any time the Contractor discovers that the Time Schedule cannot be met it will immediately advise the City in writing and provide a revised Time Schedule.

2.7 Warranty of Goods

The Contractor warrants that the Goods supplied by the Contractor shall be free from defects in design, materials, workmanship and title, shall conform in all respects to the terms of this agreement, shall be fit and suitable and perform satisfactorily for the purposes and under the conditions made known to the Contractor by the City. The Goods shall be of the best quality, if no quality is specified. This general warranty is independent of and without prejudice to any specific warranty or service guarantee offered by the Contractor or third party manufacturer or supplier of the Goods in connection with the purpose for which the Goods were purchased.

The Contractor shall assign to the City any warranty or service guarantee offered by a third party manufacturer or supplier of the Goods. Notwithstanding this assignment, if at any time up to one year from the date of delivery or installation (if applicable) the City determines the Goods or any part do not conform to these warranties, the City shall notify the Contractor within a reasonable time after such discovery, and the Contractor shall then promptly correct such nonconformity at the Contractor's expense. Goods used to correct a nonconformity shall be similarly warranted for one year from the date of installation. The Contractor's liability shall extend to all liabilities, losses, damages, claims and expenses incurred by the City caused by any breach of any of the above warranties.

Goods supplied by the City and installed by the Contractor that require Services during a product warranty period shall be serviced by the Contractor at the City’s expense.

If any Goods are installed by the Contractor, and subsequently recalled by the manufacturer of the Goods, Service costs associated with the replacement of the recalled Goods will be at the Contractor`s expense. The Contractor shall notify the City if a recall notice is issued by a Goods manufacturer.

Damage to Goods caused by a third party (i.e., motor vehicle collision) shall not be covered by any Goods warranty, and the Contractor will not be held responsible for any associated damage repair costs.

3. PERSONNEL

3.1 Qualified Personnel

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

3.2 Listed Personnel and Sub-Contractors

The Contractor will provide the Goods and Services using the professional personnel and sub-contractors as may be listed in Appendix 4 and identified by the Contractor, and the Contractor will not remove any such listed personnel or sub-contractors from the Goods and 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 Contractor's personnel or sub-contractors then the Contractor 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 Contractor will not engage any personnel or sub-contractors, or sub-contract or assign its obligations under this agreement, in whole or in part, without the prior written approval of the City.

3.5 Agreements with Sub-Contractors

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

4. LIMITED AUTHORITY

4.1 Agent of City

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

4.2 Independent Contractor

The Contractor is an independent contractor. This agreement does not create the relationship of employer and employee, a partnership, or a joint venture. The City will not control or direct the details, means or process by which the Contractor performs the Goods and Services. The Contractor will determine the number of days and hours of work required to properly and completely perform the Services. The Contractor is primarily responsible for performance of the Goods and Services and may not delegate or assign any Services to any other person except as provided for in Section 3.4. The Contractor 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 Payment for Goods and Services

The City will pay to the Contractor the fees as set out in Appendix 2 (the "**Fees**"). Payment by the City of the Fees will be full payment for the Goods and Services and the Contractor 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 Contractor will submit an invoice (the "**Invoice**") to the City requesting payment of the portion of the Fees relating to the Goods and Services provided. Each Invoice should be sent **electronically** to: surreyinvoices@surrey.ca and include the following information:
   (1) an invoice number;
   (2) the Contractor's name, address and telephone number;
   (3) the City's reference number for the Goods and 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 Contractor and any sub-contractors that have performed services during the previous month;
   (5) the percentage of the Goods and Services completed at the end of the previous month;
   (6) the total budget for the Goods and 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) if the City reasonably determines that any portion of an Invoice is not payable then the City will so advise the Contractor;

(c) 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;

(d) if the Contractor 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 Records

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

5.4 Goods not listed in Appendix 2

All replacement Goods not specifically listed in Appendix 2 but required will be supplied by the Contractor and invoiced to the City at cost plus <insert percentage discount (___%).> The Contractor shall submit, upon request by the City, actual supplier's invoices to establish the cost of the Goods.

5.5 Units of Goods and Services

The estimated units of Goods and Services in Appendix 2 are for determination of the price only. The City does not guarantee that the actual amounts of Goods and Services of any unit class will correspond even

approximately to the estimated units, but reserves the right to increase or decrease the amounts of any class or portion of the Goods and Services, or to omit portions of the Goods and Services that may be deemed necessary or expedient by the City. The Contractor shall make no claim for anticipated profits, for loss of profit, for damages, or for any extra payment whatsoever, because of any difference between the amount of actual Goods and Services furnished and the quantities stated in Appendix 2.

5.6 Personnel Hourly Rates

The personnel hourly rates in Appendix 2 shall include all overhead, profit and all small tools and other miscellaneous equipment normally required by tradesmen in their provision of the Goods and Services. No payment will be made for travel time to and from each site and such time shall not be included in the time measured for payment.

5.7 Equipment Hourly Rates

The equipment hourly rates in Appendix 2 shall include all overhead, profit and shall include operators, fuel, repairs, moving charges, etc. Time required for transportation of equipment to and from work sites within Surrey will be payable at the appropriate equipment hourly rates. Payment for time required to transport equipment into and out of the City's jurisdictional boundaries will not be payable.

5.8 Incidental Goods Supply

Goods provided to aid or assist in maintenance tasks and/or installation of new or replacement parts shall be considered incidental, and shall not be paid for separately by the City under Appendix 2.

5.9 Non-Residents

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

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

6. CITY RESPONSIBILITIES

6.1 City Information

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

6.2 City Decisions

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

6.3 Notice of Defect

If the City observes or otherwise becomes aware of any fault or defect in the delivery of the Goods or the provision of Services, it may notify the Contractor, but nothing in this agreement will be interpreted as giving the City the obligation to inspect or review the Contractor's performance with regards to delivering Goods or the provision of the Services.

7. INSURANCE AND DAMAGES

7.1 Indemnity

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

7.2 Survival of Indemnity

The indemnity described in this Contract 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 Contractor's Insurance Policies

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

(a) commercial general liability insurance on an occurrence basis, in an amount not less than five million ($5,000,000) dollars inclusive per occurrence against death, bodily injury and property damage arising directly or indirectly out of the work or operations of the Contractor, its employees and agents. The insurance will include cross liability and severability of interests such that the coverage shall apply in the same manner and to the same extent as though a separate policy had been issued to each insured. The insurance will include, but not be limited to: premises and operators liability, broad form products and completed operations, owners and contractors protective liability, blanket contractual, employees as additional insureds, broad form property damage, non-owned automobile, contingent employers liability, broad form loss of use, and personal injury. 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 Contractor 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 Contractor will provide the City with evidence of the required insurance prior to the commencement of this agreement. Such evidence will be in the form of a completed certificate of insurance acceptable to the City. The Contractor will, on request from the City, provide certified copies of all of the Contractor's insurance policies providing coverage relating to the Services, including without limitation any professional liability insurance policies. All required insurance will be endorsed to provide the City with thirty (30) days advance written notice of cancellation or material change restricting coverage. The Contractor will be responsible for deductible amounts under the insurance policies. All of the Contractor's insurance policies will be primary and not require the sharing of any loss by the City or any insurer of the City.

7.5 Contractor Responsibilities

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

7.6 Additional Insurance

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

8. TERMINATION

8.1 By the City

The City may at any time and for any reason by written notice to the Contractor terminate this agreement before the completion of all the Goods and Services, such notice to be determined by the City at its sole discretion. Upon receipt of such notice, the Contractor will perform no further Goods and Services other than the work which is reasonably required to complete the Goods and Services. Despite any other provision of this agreement, if the City terminates this agreement before the completion of all the Goods and Services, the City will pay to the Contractor all amounts owing under this agreement for Goods and Services provided by the Contractor up to and including the date of termination, plus reasonable termination costs in the amount as determined by the City in its sole discretion. Upon payment of such amounts no other or additional payment will be owed by the City to the Contractor, and, for certainty, no amount will be owing on account of lost profits relating to the portion of the Goods and 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 Contractor is adjudged bankrupt, or makes a general assignment for the benefit of creditors because of its insolvency, or if a receiver is appointed because of its insolvency,

the City may, without prejudice to any other right or remedy the City may have, terminate this agreement by giving the Contractor or receiver or trustee in bankruptcy written notice; or

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

If the City terminates this Contract 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 Goods and Services;
(b) withhold payment of any amount owing to the Contractor under this agreement for the performance of the Goods and Services;
(c) set-off the total cost of completing the Goods and Services incurred by the City against any amounts owing to the Contractor under this agreement, and at the completion of the Goods and Services pay to the Contractor any balance remaining; and
(d) if the total cost to complete the Goods and Services exceeds the amount owing to the Contractor, charge the Contractor the balance, which amount the Contractor will forthwith pay.

8.3 Curing Defaults

If the Contractor 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 Contractor, remedy the default and set-off all costs and expenses of such remedy against any amounts owing to the Contractor. 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 Contractor.

9. APPLICABLE LAWS, BUILDING CODES AND BY-LAWS

9.1 Applicable Laws

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

9.2 Codes and By-Laws

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

9.3 Interpretation of Codes

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

10. CONFIDENTIALITY AND DISCLOSURE OF INFORMATION

10.1 No Disclosure

Except as provided for by law or otherwise by this agreement, the Contractor will keep strictly confidential any information supplied to, obtained by, or which comes to the knowledge of the Contractor as a result of the performance of the Goods and 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 Goods and Services.

10.2 Freedom of Information and Protection of Privacy Act

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

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

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

10.3 Return of Property

The Contractor agrees to return to the City all of the City's property at the completion of this agreement, including any and all copies or originals of reports provided by the City.

11. USE OF WORK PRODUCT

The Contractor 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 Contractor.

12. WORKERS' COMPENSATION BOARD AND OCCUPATIONAL HEALTH AND SAFETY

12.1 The Contractor 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 the supply of the Goods and Services. The Contractor 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 Contractor. The City will have the right to withhold payment under this agreement until the Workers' Compensation Board premiums, assessments or penalties in respect of the Goods and Services have been paid in full.

12.2 The Contractor will provide the City with the Contractor's Workers' Compensation Board registration number and a letter from the Workers' Compensation Board confirming that the Contractor 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.

12.3 The Contractor agrees that it is the prime contractor for the Services as defined in the *Workers Compensation Act, R.S.B.C. 2019, c.1.* The Contractor will have a safety program in place that meets the requirements of the Workers' Compensation Board Occupational Health and Safety Regulation and the *Workers Compensation Act*. As prime contractor, the Contractor will be responsible for appointing a qualified coordinator for insuring the health and safety activities for the location of the Services. That person will be the person so identified in this agreement, and the Contractor will advise the City immediately in writing if the name or contact number of the qualified coordinator changes.

12.4 Without limiting the generality of any other indemnities granted by the Contractor in this agreement, the Contractor 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.

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

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

13. BUSINESS LICENSE

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

14. DISPUTE RESOLUTION

14.1 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 14.

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

(b) Mediation
If all or any portion of a Dispute cannot be resolved by good faith negotiations within 30 days, either party may by notice to the other party refer the matter to mediation. Within 7 days of delivery of the notice, the parties will mutually appoint a mediator. If the parties fail to agree on the appointment of the mediator, then either party may apply to the British Columbia

International Commercial Arbitration Centre for appointment of a mediator. The parties will continue to negotiate in good faith to resolve the Dispute with the assistance of the mediator. The place of mediation will be Surrey, British Columbia. Each party will equally bear the costs of the mediator and other out-of-pocket costs, and each party will bear its own costs of participating in the mediation.

(c) Litigation

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

15. JURISDICTION AND COUNCIL NON-APPROPRIATION

15.1 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.

15.2 The Contractor recognizes and agrees that the City cannot make financial commitments beyond the City's current fiscal year. The City will annually make bonafide requests for appropriation of sufficient funds to cover all payments covered by this agreement. If City Council does not appropriate funds, or appropriates insufficient funds, the City will notify the Contractor of its intention to terminate or reduce the services so affected within 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.

16. GENERAL

16.1 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 Goods and 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 Goods and Services.

16.2 Amendment

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

16.3 Contractor Terms Rejected

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

16.4 Survival of Obligations

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

16.5 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.

16.6 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 – 104 Avenue, Surrey, B.C., Canada V3T 1V8

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

Telephone No.: **<insert>**
Fax No.: **<insert>**
Email: **<insert>**

(b) The Contractor:

<insert name and address>

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

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

16.7 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.

16.8 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.

16.9 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.

16.10 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.

16.11 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.

[End of Page]

16.12 Enurement

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

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)

_____
(Print Name and Position of Authorized Signatory)

[INSERT NAME OF CONTRACTOR]

I/We have the authority to bind the Contractor.

_____
(Legal Name of Contractor)

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

(APPENDICES 1 THROUGH 7 WILL BE INSERTED LATER WHEN AN AGREEMENT IS ASSEMBLED FOR EXECUTION INCLUDING INFORMATION FROM THE RFP AND SUCCESSFUL PROPOSAL)

APPENDIX 1 – SPECIFICATIONS OF GOODS AND SCOPE OF SERVICES

APPENDIX 2 – FEES AND PAYMENT

APPENDIX 3 – TIME SCHEDULE

APPENDIX 4 – PERSONNEL AND SUB-CONTRACTORS

APPENDIX 5 – ADDITIONAL SERVICES

APPENDIX 6 – PRIVACY PROTECTION SCHEDULE

APPENDIX 7 – CONFIDENTIALITY AGREEMENT

SCHEDULE C – FORM OF PROPOSAL

RFP Project Title: **City-Wide Wi-Fi Replacement**

RFP Reference No.: **1220-030-2021-031**

Legal Name of Proponent: _____

Contact Person and Title: _____

Business Address: _____

Business Telephone: _____

Business Fax: _____

Business E-Mail Address: _____

TO:

City of Surrey

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

Email 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 Goods and Services required, and having fully informed ourselves as to the intent, difficulties, facilities and local conditions attendant to performing the Goods and 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 Technical Proposal (Services);
Schedule C-4 – Proponent's Technical Proposal (Time 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 the agreement, I/we will at all times be the "prime contractor" as provided by the Worker's Compensation Act (British Columbia) with respect to the Goods and Services. I/we further confirm that if I/we become aware that another contractor at

the place(s) of the Goods and Services has been designated as the “prime contractor”, I/we will notify the City immediately, and I/we will indemnify and hold the City harmless against any claims, demands, losses, damages, costs, liabilities or expenses suffered by the City in connection with any failure to so notify the City.

This Proposal is submitted by this **[day]** day of **[month], [year].**

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 agreement attached to the RFP as Schedule "B". If requested by the City, I/we would be prepared to enter into that agreement, 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 agreement 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 Standard Certificate of Insurance;

(d) City of Surrey or Intermunicipal business license Number: _____;

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

(f) If the Proponent 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 agreement 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) Location of primary business, branch locations, background, stability, structure of the Proponent and number of years business has been operational;

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

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

(iv) Proponent's equipment resources, capability and capacity, as relevant (including equipment resources under the Proponent's control, equipment resources to be rented, and equipment resources to be purchased);

(v) Proponent's references (name and telephone number). The City's preference is to have a minimum of three references;

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

(vii) Proponents should provide information on the background and experience of all key personnel proposed to undertake the Services (use the spaces provided and/or attach additional pages, if necessary):

Key Personnel

Name: _____

Experience:

Dates: _____
Project Name: _____
Responsibility: _____
_____
_____

Dates: _____
Project Name: _____
Responsibility: _____
_____
_____

Dates: _____
Project Name: _____
Responsibility: _____
_____
_____

Sub-Contractors

(viii) Proponents should provide the following information on the background and experience of all sub-contractors proposed to undertake a portion of the Goods and Services (use the spaces provided and/or attach additional pages, if necessary):

DESCRIPTION OF SERVICES	SUB-CONTRACTORS NAME	YEARS OF WORKING WITH PROPONENT	TELEPHONE NUMBER AND EMAIL

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

SCHEDULE C-3 - PROPONENT'S TECHNICAL PROPOSAL (SERVICES)

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

(i) a narrative that illustrates an understanding of the City's requirements for Goods and Services;

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

(iii) a narrative that illustrates how the Proponent will provide the Goods and perform the Services, and accomplish required objectives within the City's schedule;

(iv) a description of the standards to be met by the Proponent in providing the Goods and Services;

(v) a list of reports that you would anticipate providing the City's management team, including their relationship to project milestones and the method of delivery (electronic, paper, e-mail, other);

(vi) Environmental and Social Responsibility: Describe your commitment to environmental stewardship initiatives, recycling practices and carbon footprint reduction;

(vii) Value Added Services: 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. Unless otherwise stated, it is understood that there are no extra costs for these goods and services.

[End of Page]

SCHEDULE C-4 - PROPONENT'S TECHNICAL PROPOSAL (TIME SCHEDULE)

The City encourages responses that demonstrate a thorough understanding of the nature of the work and what the Proponent must do to get the work done properly. To this end, Proponents should provide an estimated project schedule, with major item descriptions and time indicating a commitment to provide the Goods and perform the Services within the time specified (use the spaces provided and/or attach additional pages, if necessary).

MILESTONE DATES _____

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

[End of Page]

SCHEDULE C-5 - PROPONENT'S FINANCIAL PROPOSAL

Indicate the Proponent's proposed fee (excluding GST), and the basis of calculation (use the spaces provided and/or attach additional pages, if necessary) as follows (as applicable):

[End of Page]

Table A: Schedule of Rates:

Site	Address	Hardware	Installation	Other	Comments	Total Amount
North						
City Hall, City Centre Library, & 3 Civic Plaza	13450 104 Avenue					
North Surrey Sports & Ice Complex	10950 126A Street					
RCMP - Whalley/City Centre District Office 1	10720 King George Boulevard					
Chuck Bailey Recreation	13458 107A Avenue					
Bridgeview Community Centre	11475 126A Street					
West Village Boiler Plant	13231 Central Avenue					
RCMP - Guildford District Office 2	10395 148 Street					
Guildford Campus - Library/Recreation/Aquatics	15105 105 Avenue					
Hemlock Operations	9353 160 Street					
Fraser Heights Recreation	10588 160 Street					
Central East						
Animal Center	17944 Colebrook Road					
Cloverdale Museum & Campus - Archives & Library	17710 56 Avenue					
RCMP - Cloverdale District Office 4	5732 176A Street					
Cloverdale Recreation & Arena	6188 176 Street					
Port Kells Library	18885 88 Avenue					
Clayton Community Center	7155 187A Street					
Clayton Hall	18513 70 Avenue					

Central West						
Fire Hall 1	8767 132 Street					
Surrey Fire Training Centre	1491 64 Avenue					
Operation Centre Administration & Fleet Buildings	6651 148 Street					
Arts Centre	13750 88 Avenue					
RCMP - Newton District Office 3	7235 137 Street					
Newton Campus - Pools/Arena/Seniors/Library	13730 72 Avenue					
Strawberry Hill Library	7399 122 Street					
Old City Hall - North Annex, RCMP, & West Wing	14355 57 Avenue					
South						
Darts Hill	1660 168 Street					
Grandview Heights Aquatics Centre	16855 24 Avenue					
South Surrey Operations Centre	16666 24 Avenue					
Semiahmoo Library	200-1815 152 Street					
Surrey Cemetery	14850 28 Avenue					
South Surrey Pool - Recreation & Arena	14655 17 Avenue					
RCMP - South Surrey District Office 5	#100-1815 152 Street					
Ocean Park Library	12854 17 Avenue					
CURRENCY: Canadian					**Subtotal:**	
					GST (5%):	
					TOTAL PROPOSAL PRICE:	

Table B: List of Optional Prices:

The following is a list of optional price(s) and forms part of this RFP, upon the acceptance of any or all of the optional price(s). The optional prices are an addition or a deduction to the Total Proposal Price and do not include GST. DO NOT state a revised Total Proposal Price.

Table B - Optional Sites						
Site	**Address**	**Hardware**	**Installation**	**Other**	**Comments**	**Total**
Holland Park - Outdoor Coverage	13428 Old Yale Rd					
Bill Reid Millennium Amphitheatre	17728 64Ave					
Newton Athletics Park (Grandstand & Park Areas)	7395 128 St					
South Surrey Athletic Park	14600 - 20 Ave					

[End of Page]

Proponents should complete the following tables setting out the all-inclusive hourly rates including overhead, profit, small tools and work vehicles (trucks/vans) for approved extras/credits for all applicable categories of labour (use the spaces provided and/or attach additional pages, if necessary):

Table C – Schedule of Labour Rates:

Labour Category	Straight Time/hr (Plus GST)	Overtime Rate/hr (Plus GST)
.1 Superintendent	$	$
.2 Foreman	$	$
.3 Journeyman	$	$
.4 Apprentice	$	$
.5 Skilled Labourer	$	$
.6	$	$

Table D – Schedule of Equipment Rates:

No.	Equipment Description	Hourly Rate
		$
		$

Additional Expenses:

The proposed Contract attached as Schedule "B" to the RFP provides that expenses are to be included within the fee, other than the expenses listed in the Contract as disbursements. Details of disbursements are to be shown in the chart above. Please indicate any expenses that would be payable in addition to the proposed fee and proposed disbursements set out above:

_____

_____

ATTACHMENT 1 – PRIVACY PROTECTION SCHEDULE

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

Definitions

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

Purpose

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

Collection of personal information

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

Accuracy of personal information

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

Requests for access to personal information

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

Correction of personal information

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

Protection of personal information

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

Storage and access to personal information

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

Retention of personal information

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

Use of personal information

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

Disclosure of personal information

16. Unless the Public Body otherwise directs in writing, the Contractor may only disclose personal information inside

Canada to any person other than the Public Body if the disclosure is for the performance of the Contractor's obligations, or the exercise of the Contractor's rights, under the Agreement.

17. Unless the Agreement otherwise specifies or the Public Body otherwise directs in writing, the Contractor must not disclose personal information outside Canada.

Notice of foreign demands for disclosure

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

(a) receives a foreign demand for disclosure;

(b) receives a request to disclose, produce or provide access that the Contractor knows or has reason to suspect is for the purpose of responding to a foreign demand for disclosure; or

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

Notice of unauthorized disclosure

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

Inspection of personal information

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

Compliance with the Act and directions

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

(a) the requirements of the Act applicable to the Contractor as a service provider, including any applicable order of the commissioner under the Act; and

(b) any direction given by the Public Body under this Schedule.

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

Notice of non-compliance

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

Termination of Agreement

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

Interpretation

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

ATTACHMENT 2 – CONFIDENTIALITY AGREEMENT

WHEREAS:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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