REQUEST FOR TENDERS

Instructions to Bidders

K1001130 & K1001131

Ft. Nelson FLNRO - Furnace & DDC Upgrade

6100 - 50th Ave. N (Mile 301 Hwy 97) Ft. Nelson

Tender Close before 2:00:00 PM Pacific Time on:

June 10, 2021 **unless specified otherwise in and Addendum to this document.**

Issued: May 12, 2021

TABLE OF CONTENTS

1. GENERAL

1.1 The intent of these Instructions to Bidders is to solicit bids to perform the Work as defined in these Bid Documents.

1.2 The project consists of (the "Project"):

The scope of work for this project is to replace 7 existing furnaces with new High Efficiency furnaces. Work includes all associated plumbing, electrical and ductwork modifications per the Issued for Tender drawings and specification issued by Falcon Engineering. In addition the project includes upgrades to the existing Delta Controls DDC system. The DDC upgrades are done under a Cash Allowance. A Cash allowance for Hazardous Materials abatement is also included in the scope of work.
The awarded Contractor will be responsible for all aspects of the work and will be required to act as the Prime Contractor for the purposes of Health & Safety on site.

A Mandatory Zoom meeting will be held to discuss the project scope. As there will be no site meeting scheduled a library of photos is available for review.
A link to the photo library will be provided by email.

1.3 Tender Period Schedule

Milestone	Date
Tender Issue	May 12, 2021
Mandatory Site Walkthrough/Teleconference	May 26, 2021
Last Day for Questions	June 3, 2021
Last Day for Addendum	June 7, 2021
Tender Close Date	June 10, 2021
Tender Close Time	2:00:00 PM PST
Estimated Notice of Award	June 15, 2021

1.4 Estimated Construction Schedule

Milestone	Date
Commence Work	August 1, 2021
Substantial Completion	September 30, 2021

1.5 Bids are by invitation only. Bids from unsolicited bidders will be returned unopened.

1.6 CONFIDENTIALITY STATEMENT: All forms, documents, E-Mails and other forms of communications, no matter the form or method of transmission, that are part of this Request for Tenders (RFT) are Confidential Information and MUST be treated as such. These forms, documents, Emails and other forms of communications, no matter the form or method of transmission, are to be used only for the specific tasks required for responding to this RFT and for performing the Work / Specific Tasks that will be defined in any "Form of Agreement" that may be issued in regards to this / these Project(s). These forms, documents, E-Mails and other forms of communications, no matter the form or method of transmission, may not be used for any other purposes and may not be shared and/or communicated in any way with any other persons, parties or entities without the express written permission of CBRE Ltd. For any documents, E-Mails and other forms of communications, no matter the form or method of transmission, that are returned to CBRE Ltd. by the Proponent, the Proponent MUST identify to CBRE Ltd. if any Confidential Information or Hyper-Links or connections of any kind to Confidential Information have been included. This is to prevent CBRE Ltd. from unknowingly distributing Confidential Information to other persons, parties or entities.

2. COMPLIANCE

2.1 The bidder acknowledges that by submitting a compliant bid, it has accepted an offer by the Owner to enter into a "bid contract" for the evaluation of bids and the award of the Contract, if an award is made. The bidder acknowledges that the terms of the "bid contract" are represented by the Bid Documents.

2.2 A bid which fails to comply with the requirements of these Instructions to Bidders may be declared non-compliant and cause the bid to be rejected.

3. BID DOCUMENTS

3.1 The basis of this bid process (the "Bid Documents") are listed in this Section 3.1. The Bid Documents include but are not limited to:

.1 Instructions to Bidders

.2 Additional Information and Requirements:

(i) CBRE Contractors HSE Guide – Province of BC

(ii) Waste Diversion & Reporting Requirements

(iii) CBRE Vendor Performance Program

(iv) CBRE Invoicing Requirements

(v) Conflict of Interest Form

(vi) Schedule B – Province of BC Required Flow Downs

.3 Agreement, Definitions and General Conditions of the CCDC2 – 2008

.4 Supplementary Conditions to CCDC 2, 2008

.5 Site Specific Work Restrictions and Special Instructions

.6 Drawings as noted in the table below:

Table 3.1.5 - Included Drawings

Drawing Numbers	Issued by	Date / Revision Number
Mechanical M1.0 - M4.4	Falcon Eng'g	Rev 2 - Issued for Tender April 19-2021
Electrical E1- E4	Falcon Eng'g	Rev 1 Issued for Tender April 9, 2021

.7 Equipment Inventory form (sample document)

.8 Construction Waste form (sample document)

.7 Specifications as noted in the table below: (examples shown)

Table 3.1.6 - Included Specifications		
Divisions	Issued by	Date / Revision Number
Division 20 - Mechanical	Falcon Eng'g	Issued for Tender April 13, 2021

.8 Addenda issued during bidding period.

3.2 Upon receipt of the Bid Documents, the bidders shall check the Bid Documents for completeness. Bidders shall inform the Bid Coordinator identified in Section 8 of these Instructions to Bidders immediately:

.1 should any documents be missing or incomplete;

.2 upon finding any discrepancies or omissions.

3.3 Examine and read the Bid Documents thoroughly. It is the responsibility of the bidder to check all drawings, specifications, schedules and Addenda prior to the submission of the bid.

3.4 Complete sets of Bid Documents are issued electronically to all bidders.

3.5 The Bid Documents are made available only for the purpose of submitting bids for the Project. Availability and/or use of the Bid Documents do not confer a licence or grant for any other purpose.

3.6 Except as otherwise defined in these Instructions to Bidders, the defined terms in these Bid Documents are taken from the Contract. The term Contract is defined in the Agreement.

4. CONDITIONS OF THE PLACE OF THE WORK

4.1 The following reports prepared or obtained with respect to the Place of the Work are included in the Bid Documents listed in Section 3.1.

4.2 Before submitting a bid, investigate the Place of the Work to fully ascertain existing conditions, circumstances and limitations affecting the Work. No allowances will be made for additional costs and no claims will be entertained in connection with conditions which could reasonably have been ascertained by such investigation or other due diligence prior to submitting a bid.

4.3 Where the Work is to be carried out in an existing building:

.1 All onsite activities must be co-ordinated with management of the building. Bidders are responsible to adhere to all building management construction regulations from the building manager as listed in Appendix I.

.2 Bidders must include in their bid price any additional costs required due to complying with building regulations imposed by building management. These include but are not limited to deliveries, hoisting, noise, safety, clean-up, shut-downs, security, garbage removal, access, smoking, parking, site storage, washrooms, identification, site signs, designated materials, temporary services, hoarding and loading.

4.4 Any toxic or hazardous substances known to exist at the Place of the Work are identified in the reports as noted in Section 3.1.

4.5 The Owner promotes environmentally responsible products and working practices, typically compatible with the property owner's objectives, most of whom have existing corporate environmental policies.

4.6 The Owner expects the Bidder, its Suppliers and Subcontractors to take into consideration the environmental impacts of their products and working practices. The Bidder, its Subcontractors and Suppliers should consider packaging materials, waste factors and disposal practices, demonstrating environmental responsibility.

5. EXAMINATION OF SITE / MANDATORY SITE MEETING

5.1 Before submitting a bid, bidders must examine the Project Site and surroundings to satisfy themselves as to the existing conditions and limitations of the Project Site, the means of access to the same and the nature and quantity of work required.

5.2 No adjustments to the Project schedule or to the price of the Contract entered into with a successful bidder will be made for difficulties encountered due to conditions, features or peculiarities of the Place of the Work which exist and are known, reasonably discernable or visible at the time of the Bid.

5.3 A MANDATORY TELECONFERENCE will be held and Proponents MUST attend. All Proponents MUST arrive on time and MUST stay for the entire Mandatory Teleconference. Any Proponent that arrives late or does not stay for the entire Mandatory Teleconference will be asked to leave the Teleconference and Will Be Disqualified. Any Proponent deemed disruptive to the Mandatory Teleconference by CBRE will be asked to leave the Teleconference and May be Disqualified.

If a Non-Disclosure Agreement (NDA) is required as part of this Project, the Proponent MUST supply a properly completed and properly executed (including a signature from an officer of the Proponent's firm) NDA to the CBRE Representative listed below before the start of the Mandatory Teleconference. If a properly completed and properly executed NDA is not provided to the CBRE Representative listed below the Proponent will be asked to leave the Teleconference and Will Be Disqualified.

If two (2) or less Proponents attend this Mandatory Teleconference CBRE reserves the right to stop this Teleconference and, via an Addendum, reschedule the Mandatory Teleconference to a different date and / or time.

The Mandatory Teleconference will be held: May 26, 2021 at 10:00 am

The teleconference number for this call will be: TBA. Zoom invitation to follow

All attendees MUST ensure that they register their name and title as well as their company name with conference Chair and CBRE Representative, Iris Anderson.

The Purpose of this teleconference is to provide Proponents with a briefing of the project scope and expectations including, but not limited to security requirements, access, movement throughout the facility etc.

Proponents and their sub-trades may review the site located at 6100 - 50th Ave N Ft Nelson, ~~during a scheduled site visit, or~~ upon request. The purpose of a site visit is to become familiarized with the requirements governing the Work including the daily activities of the building occupants, security requirements and surrounding properties prior to submitting a response to this bid. Proponents may either attend personally or through a representative. This will allow Proponents to determine the nature and location of the Work, local conditions, soil structure and topography at the site of the Work, the equipment and facilities needed preliminary to and during the prosecution of the Work, the means of access to the site, on-site accommodation, all necessary information as to risks, contingencies and circumstances, which may affect the response to this bid, and all other matters which can in any way affect the Work. Proponents are fully responsible for obtaining all information required for the preparation of their response to this bid.

5.4 ~~A MANDATORY SITE VISIT at will be held and Proponents MUST attend. All Proponents MUST arrive on time and MUST stay for the entire Mandatory Site Visit. Any Proponent that arrives late or does not stay for the entire Mandatory Site Visit Will be Disqualified. Any Proponent deemed disruptive to the Mandatory Site Visit by CBRE will be asked to leave the Site Visit and may be Disqualified.~~

~~**Mandatory Site Visit Details**~~
~~Address:~~
~~Time:~~
~~Location Details:~~

~~All Proponents are to ensure that they register their name and title as well as their company name with the CBRE Representative, _____.~~

If a Non-Disclosure Agreement (NDA) is required as part of this Project, the Proponent MUST supply a properly completed and properly executed (including a signature from an officer of the Proponent's firm) NDA to the CBRE Representative listed below before the start of the Mandatory Site Visit or when they arrive at the Mandatory Site Visit. If a properly completed and properly executed NDA is not provided to the CBRE Representative listed below the Proponent will be asked to leave the Site Visit and Will Be Disqualified.

~~If two (2) or less Proponents attend this Mandatory Site Visit CBRE reserves the right to stop this Site Visit and, via an Addendum, reschedule the Mandatory Site Visit to a different date and / or time.~~

~~During a Mandatory Site Visit Proponents MUST Not use any electronic device (i.e. Laptop PC, Smart Phone, Cell Phone, PDA, etc.) except to take notes. Proponents are prohibited from making and / or receiving telephone calls and transmitting and / or receiving data / information / messages on any electronic device. This includes sending and / or receiving E-Mails and sending and / or receiving any electronic messaging. A proponent that does not comply with this Mandatory Requirement will be deemed as disrupting the Mandatory Site Visit, will be asked to leave the Site Visit and may be Disqualified.~~

~~Proponents and their sub-trades may review the site during this scheduled site visit. The purpose of a site visit is to become familiarized with the requirements governing the Work including the daily activities of the building occupants, security requirements and surrounding properties prior to submitting a response to this bid. Proponents may either attend personally or through a representative. This will allow Proponents to determine the nature and location of the Work, local conditions, soil structure and topography at the site of the Work, the equipment and facilities needed preliminary to and during the prosecution of the Work, the means of access to the site, on-site accommodation, all necessary information as to risks, contingencies and circumstances, which may affect the response to this bid, and all other matters which can in any way affect the Work. Proponents are fully responsible for obtaining all information required for the preparation of their response to this bid.Bids received from bidders who failed to attend the mandatory site meeting, as determined from the "Site Meeting Log", will be returned unopened.~~

5.5 In its sole and absolute discretion, CBRE may schedule additional site meetings. Should additional site meetings be scheduled, all bidders shall be notified of the time, date and location for the additional meetings. In the event that a bidder has attended the first mandatory site meeting, it is at their discretion to attend any subsequent meeting.

6. PREQUALIFICATION

6.1 Bidders must use Subcontractors and Suppliers from the following prequalified list for each of the prescribed trade disciplines:

Table 6.1 - Approved Subcontractors		
Discipline	Company Name	Contact
DDC - Controls	Inland Control & Services Inc.	Adam Norn - 250-563-6886

6.2 Bidders who fail to comply with 6.1 shall be declared non-compliant and cause the bid to be rejected.

7. BID AND PERFORMANCE SECURITY

7.1 Each bid shall be accompanied by bid security in the form of a bid bond in the amount equal to ten percent (10%) of the Bid Price naming the Owner and CBRE Limited as dual obligees and issued by a surety licensed to conduct surety and insurance business in the jurisdiction of the Project. The bid security is for the benefit of the Owner and stands as security that the bidder, if awarded the Contract, will deliver the performance security and evidence of insurance and other documents required by these Instructions to Bidders or by the Contract, and will execute the Contract. The bid security shall remain valid for a period of ninety (90) days from the date of bid submission. No other form of bid security is acceptable.

7.2 The bid security of the bidder whose bid is accepted will be retained by the Owner to compensate the Owner for the damages it will suffer should the successful bidder fail to execute the Contract and/or fail to provide the specified performance security and/or evidence of insurance and other documents required by these Instructions to Bidders or by the Contract.

7.3 Each Bid shall be accompanied by an agreement to bond issued by a surety company licensed to conduct surety and insurance business in the jurisdiction of the Project, undertaking to provide a fifty percent (50%) performance bond and a fifty percent (50%) labour and material payment bond, both to be delivered to the Owner if the Bidder is awarded the Contract.

7.4 Bids not accompanied by the required agreement to bond will be declared non-compliant and rejected.

7.5 Include the cost of all bonds in the bid price.

8. QUESTIONS ARISING DURING BIDDING

8.1 Direct questions arising during the bidding period to the Bid Coordinator:

Name: Iris Anderson Phone: 778-349-4504

Email: iris.anderson@cbre.com

8.2 The Bid Coordinator is the sole contact for bidding on this Project. A bid may be disqualified where contact is made with any person other than the Bid Coordinator. Questions may be submitted directly to the Bid Coodinator using the above contact information, ~~or submitted through the Kahua Bid Management tool.~~

8.3 If bidders find discrepancies, omissions, errors, departures from building by-laws, codes or good practice, and points considered to be ambiguous or conflicting, they shall bring them to the attention of the Bid Coordinator in writing, and not less than five (5) Working Days before the bid closing date, so that the Consultant may, if the Consultant deems it necessary, issue instructions, clarifications or amendments by addendum to all bidders through the Bid Coordinator prior to the bid closing date. The Bid Coordinator will endeavour to issue such addenda at least forty-eight (48) hours prior to bid closing.

9. AMENDMENTS TO BID DOCUMENTS

9.1 The Bid Coordinator reserves the right to issue instructions and Addenda during the bid period by electronic transmission.

9.2 Neither the Owner nor CBRE nor the Consultant will be responsible for instructions, clarifications or amendments communicated orally. Instructions, clarifications or amendments which affect the Bid Documents may only be made by addendum.

9.3 Addenda issued during the bidding period shall become part of the Bid Documents and their receipt shall be acknowledged in the space provided on the Bid Form. Failure to acknowledge the receipt of Addenda may render the bid submission invalid and cause the bid to be rejected. Addenda will be sent to all bidders.

9.4 Failure to provide any additional information requested in an Addendum may result in the Bid being declared as nonconforming and cause the bid to be rejected.

10. TAXES

10.1 The Goods and Services Tax (GST), value added taxes or Harmonized Sales Tax (HST) as appropriate in the jurisdiction of the Place of the Work shall not be included in the bid price. All other eligible taxes shall be included in the bid price. Any taxes or increases to taxes announced prior to the date of the issuance of the Bid Documents and scheduled to come into effect subsequent to it shall be taken to be included in the bid price.

11. BID COMPLETION

11.1 Fill in all blank spaces on the Bid Forms and Appendices (Supplementary Bid Forms) ~~within Kahua Bid Room~~ as required, and submit PDFcopies of the provided forms in this document. Failure to provide all requested information on the Bid Forms and failure to fill in all blank spaces may result in a bid being declared non-compliant and cause the bid to be rejected.

11.2 The bid will be considered to be authorized and executed once the bid has been emailed to the Bid Coordinator as directed by the Project Manager. Submissions may be updated or resubmitted until the Bid Due Date and Time expiry.

11.3 Use only the Bid Forms issued as part of the Bid Documents for the Project, ~~or as available within Kahua Bid Room~~. If any or all pages of the Bid Forms are amended by addendum, only the amended pages shall be used to submit a bid. Failure to comply with this paragraph may result in the bid being declared non-compliant.

11.4 Information provided by bidders on the Bid Forms may be amended prior to bid closing, provided corrections are initialled by an authorized representative of the bidder. Other modifications, erasures, additions, conditions, qualifications or un-initialled pre-closing amendments may result in the bid being declared non-compliant.

11.5 Bids that are incomplete, conditional or illegible, may be declared non-compliant.

11.6 Bid Price

.1 The Base Bid Form provides that the bid price shall be provided in numbers within the bid form ~~or in fields indicated in Kahua Bid Room.~~

.2 Where the Bid Forms require the bidder to provide a breakdown of the bid price, the bid price shall govern in the case of conflict or ambiguity between the bid price and the sum of the breakdown of the bid price. Bidder is responsible for ensuring their total Bid Price is accurate once all line items are completed.

11.7 Listing of Subcontractors

.1 Where required by the Bid Documents, a bidder shall complete and submit a Supplementary Bid Form – List of Subcontractors, naming the Subcontractors and Suppliers which the bidder will employ to perform an item of the Work called for by the Contract. Failure of the bidder to list Subcontractors and Suppliers, where required, or the listing by a bidder of more than one Subcontractor and Supplier to perform or supply an item of work listed, may result in the bid being declared non-compliant.

.2 Where a bidder lists "own forces" in lieu of a Subcontractor, the bidder shall carry out such item of the Work with its own forces. Where "own forces" have been listed by a bidder, the Owner reserves the right to obtain information from the bidder and from third parties respecting the qualifications and experience of the bidder's "own forces" for such item of the Work. If the Owner, acting reasonably, determines that the bidder's "own forces" are not sufficiently qualified or sufficiently experienced to undertake such item of the Work, it may reject the bid.

.3 No changes to the list of Subcontractors will be permitted prior to award of the Contract without the prior written consent of the Owner. The Owner reserves the right, before award of the Contract, to reject a Subcontractor or Supplier proposed by a bidder. In such event, the bid price of the bidder will be adjusted by the net difference between the amount quoted to the bidder by the rejected Subcontractor and the quote of the replacement Subcontractor.

.4 Where stipulated in the Specifications or indicated on a Drawing, the Owner reserves the right, either before or after the award of the Contract, to assign to the Contractor all or portions of any contract procured by the Owner as more particularly described in GC3.7 of the General Conditions, as amended by the Supplementary Conditions. In the event of such an assignment, the Contractor may apply a mark-up of no more than 5%.

11.8 Itemized Prices. Where required by the Bid Documents, a bidder shall complete the Itemized Prices section within Kahua Bid Room.

.1 Itemized Prices for work, if any, shall be included in the Bid Price.

.2 All Itemized Prices submitted take into consideration and allow for changes and adjustments in other work as may be necessary to provide a finished and functional result, unless specifically indicated otherwise.

.3 Itemized Prices shall be the bidder's price for a specific item of work included in the Bid Price.

.4 Bidders shall submit Itemized Prices within twenty-four hours of receipt of a request from CBRE.

.5 Itemized Prices are provided for information only. They will not be used to adjust the scope of the work or the bid price.

.6 Itemized Prices do not include the Goods and Services Tax (GST), applicable value added taxes or Harmonized Sales Tax (HST) as appropriate in the jurisdiction of the Place of the Work. All other eligible taxes are included.

11.9 Alternative Prices. Where required by the Bid Documents, a bidder shall complete the Alternative Prices section within Kahua Bid Room.

.1 Alternative Prices for work, if any, shall not be included in the Bid Price.

.2 All Alternative Prices submitted take into consideration and allow for changes and adjustments in other work as may be necessary to provide a finished and functional result, unless specifically indicated otherwise.

.3 All Alternative Prices submitted include the cost of all: labour, materials, equipment, mark-ups, overheads, profit, direct and indirect supervision and represent the net cost to the Owner.

.4 Alternative Prices for work shall be stipulated as an addition, a deletion or no change to the Bid Price.

.5 The Owner reserves the right to accept or reject any of the Alternative Prices. If the Owner chooses to accept any of the Alternative Prices they will be added or deducted from the Bid Price to arrive at a final award amount. Acceptance of Alternative Prices is subject to the earlier acceptance of the bid or the bid expiry date.

.6 The Bid Documents identify the Alternative Prices requested as part of the Bid.

.7 The Owner reserves the right to accept or reject any or all alternative prices submitted.

.8 Alternative Prices do not include the Goods and Services Tax (GST), applicable value added taxes or Harmonized Sales Tax (HST) as appropriate in the jurisdiction of the Place of the Work. All other eligible taxes are included.

11.10 Separate Prices. Where required by the Bid Documents, a bidder shall complete the Separate Prices section within Kahua Bid Room.

.1 A Separate Price is a price for a particular article or item of work not included in the bid price and shall be added to or deducted from the Bid Price in accordance with the Bid Documents, if accepted.

.2 All Separate Prices submitted take into consideration and allow for changes and adjustments in other work as may be necessary to provide a finished and functional result, unless specifically indicated otherwise.

.3 All Separate Prices submitted include the cost of all: labour, materials, equipment, mark-ups, overheads, profit, direct and indirect supervision and represent the net cost to the Owner.

.4 The Owner reserves the right to accept or reject any of the Separate Prices. If the Owner chooses to accept any of the Separate Prices they will be added or deducted from the Bid Price to arrive at a final award amount. Acceptance of Separate Prices is subject to the earlier acceptance of the bid or the bid expiry date.

.5 The Bid Documents identify the Separate Prices requested as part of the Bid.

.6 The Owner reserves the right to accept or reject any or all Separate Prices submitted.

.7 Separate Prices do not include the Goods and Services Tax (GST), applicable value added taxes or Harmonized Sales Tax (HST) as appropriate in the jurisdiction of the Place of the Work. All other eligible taxes are included.

11.11 Unit Prices. Where required by the Bid Documents, a bidder shall complete the Unit Prices section within Kahua Bid Room.

.1 Unit Prices shall be for specific measurable units of material and labour. All unit prices, unless specifically indicated, are for complete work, in place, supplied and installed in accordance with applicable Contract requirements and include all overhead and profit mark-up.

.2 Credits for deleted work shall be no less than eighty-five percent (85%) of the submitted Unit Prices.

.3 The Owner shall have the right to negotiate the cost of additional work instead of using the submitted Unit Prices.

.4 Submitted Unit Prices include the cost of all: labour, materials, equipment, mark-ups, direct and indirect supervision.

.5 Unit Prices do not include the Goods and Services Tax (GST), applicable value added taxes or Harmonized Sales Tax (HST) as appropriate in the jurisdiction of the Place of the Work. All other eligible taxes are included.

11.12 Bidders Proposed Alternates. Where required by the Bid Documents, a bidder shall complete and submit a Supplementary Bid Form – Bidder Proposed Alternates. Bidders are requested to provide any voluntary alternates, which reduce the cost of the bid price without compromising the quality of the final product.

.1 All Bidder Proposed Alternates will be examined by the Owner and the Consultant and are subject to review and acceptance. The Owner may in its sole and absolute discretion accept any Bidder Proposed Alternates he deems acceptable.

.2 All Bidder Proposed Alternates submitted must take into consideration and allow for changes and adjustments in other work as may be necessary to provide a finished and functional result, unless specifically indicated otherwise.

.3 All submitted Bidder Proposed Alternates include the cost of all: labour, materials, equipment, mark-ups, overheads, profit, direct and indirect supervision and represent the net cost to the Owner.

.4 Without limiting its rights under the Instructions to Bidders, the Owner reserves the right to accept or reject any of the Bidder Proposed Alternates. Acceptance of Bidder Proposed Alternates is subject to the earlier acceptance of the bid or the bid expiry date.

.5 Bidder Proposed Alternates do not include the Goods and Services Tax (GST), applicable value added taxes or Harmonized Sales Tax (HST) as appropriate in the jurisdiction of the Place of the Work. All other eligible taxes are included.

.6 The submission of Bidder Proposed Alternates is not a requirement of the Bid.

11.13 Key Personnel. Where required by the Bid Documents, a bidder shall complete and submit a Supplementary Bid Form – Key Personnel, which shall list the names of the bidder's key personnel to be assigned to the Project.

11.14 None of the offices or facilities of the Owner, CBRE, the Consultant, the building landlord and/or the occupier of the Place of the Work may be used during the preparation of bids (ie. reception area, chairs, telephones, facsimile machines or other devices).

12. BID SUBMISSION

12.1 Submit ~~electronic Kahua Bid Room form where applicable and~~ one (1) PDF copy (where the submission is not a Kahua Bid Room function) of the following documents:

The Base Bid Form
The bid bond and agreement to bond as described in Sections 7.1 & 7.3
List of Subcontractors
Itemized Prices
Unit Prices
Alternative Prices
Separate Prices
Bidder Proposed Alternatives
Cash Allowances
Conflict of Interest form

12.2 Bids are to be submitted in PDF format via email.

12.3 Bids must be received by no later than 2:00:00 P.M. local time on DATE: 6/10/21 .

The time of receipt of bids shall be deemed to be the date and time indicated ~~by Kahua or by~~ CBRE's email server if bid is conducted through email. The term "local time" shall mean the time as measured by the identified ~~by Kahua or~~ CBRE's email server at the recipient's location.

12.4 ~~Bids will be date and time stamped by Kahua. Late bids will not be considered. Bidders will be responsible for ensuring they have access to Kahua and understand the process for submission.~~

12.5 Bids which are submitted by phone, facsimile transmission or by mail will not be considered.

12.6 Bidders are solely responsible for the timing of delivery of their bids.

13. BID EXPIRY PERIOD

13.1 Bids shall be irrevocable for a period of ninety (90) days from the date of submission, after which period the bid expires.

13.2 The expiry of the bids may be extended beyond the period of ninety (90) days from the date of submission at the mutual written consent of the parties.

14. BID OPENING AND EVALUATION

14.1 Bids will be opened in private.

14.2 If according to the Owner's procurement policy requirements an insufficient number of bids is received then CBRE may in its sole discretion, elect to open the bids or return them to the bidders unopened.

14.3 The Owner may reject the lowest or any bid or part of any bid, reject all bids or cancel this bid process in whole or in part.

14.4 The bid price offered on the Base Bid Form will be considered the bidder's "Base Bid".

.1 The Owner shall consider the submitted Alternative Prices, for those Alternatives that it chooses to accept, in making a determination for award.

.2 The Owner shall consider the submitted Separate Prices, for those Separate Prices that it chooses to accept, in making a determination for award.

14.5 The Owner reserves the right to award the Contract to the bidder which submitted the bid which, in the Owner's sole discretion, provides the best value to the Owner based on the criteria described in the Bid Documents including, but not limited to, a bidder's:

.1 Base Bid.

.2 Base Bid as adjusted by the Owner pursuant to the Bid Documents.

.3 Bid Price Breakdown.

.4 Information provided pursuant to Article 15 [Requests for Information].

14.6 The Owner reserves the right to award the Contract to a bidder which, in the Owner's discretion, has submitted a substantially compliant bid. Incomplete or conditional bids may be declared non-compliant.

14.7 Should the Owner receive no compliant bids, the Owner, in its discretion, may re-bid the Project or may negotiate a Contract for the whole or any part of the Project with a bidder which has submitted a non-compliant bid.

15. REQUESTS FOR INFORMATION

15.1 The Bid Coordinator may contact any one or more bidders to request information without any obligation to contact or request the same information from any other bidder or bidders.

15.2 Submission of an unbalanced or front-end loaded breakdown may result in the bid being rejected.

15.3 Within five (5) Working Days of notification by the Bid Coordinator, a bidder shall submit a preliminary construction schedule. Such preliminary construction schedule shall be consistent with the time for Substantial Performance of the Work stated in the Bid Documents. Such preliminary construction schedule may be in bar chart format and shall include all major subtrades and show Project milestones and critical schedule items, such as start and completion of major Project components.

15.4 A bidder shall submit additional information promptly if requested by the Bid Coordinator. Failure to do so may result in the bid being rejected.

15.5 Requests for a breakdown of the bid price, a preliminary construction schedule, or other requests for information shall not be construed as acceptance of a bid.

16. SUBSTITUTIONS

16.1 Any product or material utilized without approval will have to be removed from the Place of the Work and replaced with that specified at no extra cost to CBRE or the Owner.

17. AWARD OF CONTRACT, EXECUTION OF THE CONTRACT AND DOCUMENTS TO BE DELIVERED

17.1 Bidders shall not issue or make any statements or news release concerning their bid, the bid process, the Owner's evaluation of the bids, or the Owner's award or cancellation of the bid process without the express written consent of the Owner.

17.2 Prior to commencing the Work, the Contractor shall deliver to the Owner:

.1 the performance bond and the labour and material payment bond described in the Bid Documents, the form of such bonds to comply with the requirements of the Contract;

.2 certified true copies of the insurance policies required by the Bid Documents; and

.3 a current Clearance Certificate issued by the authority governing workplace safety and insurance in jurisdiction of the Place of the Work.

17.3 The Contractor shall execute the Contract and deliver the executed original to the Owner within ten (10) Working Days of receipt from the Bid Coordinator or other representative of CBRE or the Owner.

18. SCHEDULING OF THE WORK

18.1 The Successful Bidder shall be required to start work immediately upon the execution of the Contract.

18.2 It is understood that the Bid includes all costs on account of premium time or overtime required and all costs on account of premium prices required in order to obtain labour,

plant, materials or equipment or other critical items including waiting time, double handling, after hours delivery and installation, protection of new and existing services at the site in order to meet the completion dates of the scope of work and the project completion date.

18.3 It shall be understood and agreed that the Bid includes all costs on account of schedule interfacing, coordination and cooperation with other contractors or subcontractors who will be carrying out work during the progress of this contract in order to meet the completion date for the work and the overall completion date of the project.

18.4 CBRE will not entertain hardship claims or tolerate delays and interruptions in the work.

19. METHODS OF PROCEDURE

19.1 All Work that interfaces with the existing building systems or Work that occurs within Critical Areas within the building, which include but are not limited to: IT spaces, UPS Rooms, Electrical Rooms, Mechanical Rooms, and Fire Safety Rooms require the production of a Methods of Procedure (MOP) document that must be submitted to CBRE and the Consultant for review and approved by the Owner.

19.2 Bidders are responsible for the production of all Methods of Procedure documents necessary to complete the work. Bidders shall, as part of their Base Bids, include all costs associated with the production and revision of Methods of Procedures documents. The Bidder is responsible for all required revisions the Methods of Procedures documents so that they meet the approval of the Owner.

20. CONSTRUCTION BY OWNER OR OWNER'S OTHER CONTRACTORS

20.1 The Owner under separate contracts may have engaged certain vendors to perform work at the Place of the Work, which shall be completed prior to Substantial Performance. These vendors include but are not limited to:

Vendor Name	Responsibility

20.2 Bidders shall include as part of their base bids, all costs for the duration of the Project, until Total Performance of the Work, to be solely responsible for, and have overall responsibility, for construction health and safety at the Site, for compliance with all Codes

relating to construction health and safety and for maintaining and supervising all health and safety precautions and programs (including with respect to the Work and the other work performed by Owner and those vendors engaged by the Owner under separate contracts).

20.3 Bidders shall ensure that, prior to being granted access to the Place of the Work, each of the contractors engaged by the Owner under separate contract has signed and understood the health and safety compliance form included as an appendix to the supplementary conditions of the CCDC 2, 2008.

20.4 Without limiting the generality of any other provision that is contained in the contract or supplementary conditions, Bidders shall be, and shall carry out the duties and responsibilities of, the constructor", "prime contractor", "principal contractor", or similar applicable term in the province or territory of the *Place of the Work* as well as the duties and responsibilities of the "employer" or similar applicable term in the province or territory of the *Place of the Work*, all of which is within the meaning of the occupational health and safety legislation applicable to the *Place of the Work*, with respect to the Project, until Total Performance of the Work.

21. OWNER'S EQUIPMENT

21.1 The Owner may at its discretion pre-purchase certain equipment with respect to this Project. Upon award to the successful bidder, the Owner may, through a change order to the Contract, assign the pre-purchased equipment to the Contractor. Pursuant to Section 11.7.4 of these Instructions to Bidders, the successful bidder shall be entitled to a mark up of no more than five percent (5%) on the pre-tax value of the equipment.

21.2 Upon assignment, the successful bidder shall assume full responsibility for all aspects of the pre-purchased equipment, which shall include but not be limited to:

.1 Delivery of equipment to site;
.2 Unloading of equipment;
.3 Storage of equipment;
.4 Completeness of shipment;
.5 Conformance of equipment to the agreed specification;
.6 Damages to equipment;
.7 All payments to the equipment supplier.

For greater certainty, upon assignment to successful bidder, through a Contract change order, the Owner shall have no further obligations to any party with respect to the pre-purchased equipment.

22. SUBSTANTIAL PERFORMANCE OF THE WORK

22.1 The Contractor shall submit, no later than ten (10) business days prior to submitting the application for Substantial Performance of the Work, all guarantees, warranties, certificates, testing and balancing reports, distribution system diagrams, as-built drawings and specifications, spare parts, maintenance manuals and any other material or

documentation required to be submitted under the Contract together with written proof acceptable to the Owner and the Consultant, that the Work has been substantially performed in conformance with the requirements of municipal, government and utility authorities having jurisdiction. Failure to submit all the forgoing material and documentation in conformance with the Contract shall be grounds for the Consultant to reject the Contractors application for Substantial Performance of the Work.

23. COST AND EXPENSE

23.1 CBRE and the Owner are not liable to reimburse or compensate the Bidders in any manner whatsoever or under any circumstances (including, without limitation, cancellation of this Tender or the Project or the exercise of any other right by CBRE or the Owner) and CBRE and the Owner are not liable for any expenses or costs incurred by the Bidders in connection with, or in relation to, this Bid (including, without limitation, the preparation and submission of their Bids, site visits, conference calls, travel expenses, meetings, discussions and any additional information requested by CBRE or the Owner) and such expenses or costs shall be borne by the Bidders.

23.2 CBRE or the Owner shall not be responsible for any liabilities, costs, expenses, losses or damages (including, without limitation, loss of profits and loss of reputation) incurred, sustained or suffered by any Bidder in connection with this Tender in any manner whatsoever or under any circumstance (including, without limitation, prior to, subsequent to, or by reason of the Bidder's preparation or submission of the Bid or acceptance, or non-acceptance by CBRE of any Bid, or by reason of any delay in the acceptance of a Bid or cancellation of this Tender or the Project or any actions taken by CBRE or the Owner).

24. DISPUTES

24.1 Disputes arising in connection with this bid process including, without limitation, a dispute concerning the existence of the "bid contract" or a breach of the "bid contract", or a dispute as to whether the bid of any bidder was submitted on time or whether a bid is compliant, shall be dealt with by the Bidder and the Owner according to the process set forth in this Section 24.

24.2 In the event of a dispute as noted in Section 26.1 the Bidder shall give written notice to the Owner within fifteen (15) working days of the date of the bid closing. Written notice shall be delivered in hard copy to the Bid Coordinator at the address noted in Section 12.4 of these Instructions to Bidders. The responding party shall send a notice of reply within ten (10) Working Days after receipt of such notice of Dispute setting out particulars of this response.

24.3 Within ten (10) Working Days following receipt of a responding party's notice of reply under Section 26.2, the representatives for the Owner and the Bidder shall attempt to reach a reasonable resolution of the dispute in an expeditious manner. In the event that any dispute cannot be resolved by the representatives in an expeditious manner then the dispute shall be referred to the appropriate executives of the Owner and the Bidder for negotiation and resolution. Either the Owner or the Bidder may initiate such referral to the executives by notice.

24.4 Executives of the Owner and the Contractor shall meet at a mutually agreeable location within ten (10) Working Days after delivery of the notice pursuant to Section 26.3 and, thereafter, as often as they deem necessary to exchange relevant information and to attempt to resolve the dispute.

24.5 If the dispute has not been resolved within thirty (30) Days after delivery of the notice pursuant to Section 26.3, or if the executives of the Owner and the Contractor fail to meet within the ten (10) Working Day period, then either the Owner or the Bidder may refer the dispute to the courts or, if they both agree, to some other form of dispute resolution including arbitration.

24.6 Upon agreement by the Owner and the Bidder as set forth in Section 26.5 to refer the dispute to arbitration the dispute shall be referred to a confidential binding arbitration pursuant to the Arbitration Act, 1991, as amended, before a single arbitrator with knowledge of procurement/bidding law. In the event that the dispute is referred to arbitration, the Bidder agrees and the Owner agrees that they are bound to arbitrate such dispute.

24.7 In the event the dispute is referred to binding arbitration, the Owner may give notice of the dispute to one or more of the other bidders who submitted bids, whether or not they may be compliant, each of whom shall be a party to and shall be entitled to participate in the binding arbitration, and each of whom shall be bound by the arbitrator's award, whether or not they participated in the binding arbitration.

24.8 In the event the dispute is referred to binding arbitration, the parties to the arbitration shall exchange brief statements of their respective positions on the dispute, together with the relevant documents, and submit to a binding arbitration hearing which shall last no longer than two days, subject to the discretion of the arbitrator to increase such time. The parties further agree that there shall be no appeal from the arbitrator's award.

24.9 This Article is not intended to form part of any "bid contract" that may come into being between a Bidder and any prospective Subcontractor or Supplier of that Bidder.

24.10 It is agreed that no act by either party shall be construed as a renunciation or waiver of any of his rights or recourses, provided he has given the notices in accordance with this Section 24 and has carried out the instructions as provided in this Section 24.

25. CONFIDENTIALITY

25.1 The bidder acknowledges and agrees that all material and information which has or will come into the possession or knowledge of the bidder, its officers, employees and agents in connection with this bid, is confidential and proprietary data, the disclosure of which to, or the use by third parties, is strictly prohibited. The bidder agrees to hold such material and information in the strictest confidence, not to make use of it other than preparing the bid, to release it only to employees, agents and Subcontractors requiring such information and not to release or disclose it to any other party.

25.2 Unsuccessful bidders shall return their Bid Documents to the Owner within seven (7) calendar days of being advised that their bid was not successful.

26. CONFLICT OF INTEREST

26.1 Only one of a bidder's related, associated or affiliated companies or businesses shall be permitted to submit a bid for the Project.

26.2 All bidders must agree to the following as conditions of bid submission:

.1 that no person either natural or body corporate, other than the bidders has or will have any interest or share in this bid or in the proposed agreement.

.2 there is no collusion or arrangement between the bidder and any other bidder(s) in connection with this Bid.

.3 the bidder has no knowledge of the contents of other bids and has made no comparison of figures or agreement or arrangement, express or implied, with any other party in connection with the making of the bid.

END OF DOCUMENT

All contractors must report to the building admin when arriving on site.

CBRE Facility Management will assign storage locations for the contractor's equipment and materials.

Contractor will arrange for their own containers for demolition debris. Building dumpsters shall not be used.

CBRE requires the contractor to track waste and to recycle demolition materials as much as possible.

Noisy work and work that creates dust, odors or other disruptions is to be carried out during non-operational hours.

Building COVID protocols are to be followed at all times.

PROJECT NUMBER: K1001130 & K1001131

RFT – PROJECT NAME: Ft. Nelson FLNRO - Furnace & DDC Upgrade

APPENDIX A – FINANCIAL SUBMISSION REQUIREMENTS

1. All prices, fees and costs must be in Canadian dollars.

2. This Appendix is to be returned as the Financial Submission

3. The contents of this Appendix will form part of the Final Agreement negotiations.

4. All costs included in this Appendix are all inclusive and no additional factors or premiums will apply.

5. All costs included in this Appendix exclude value added taxes.

6. All costs provided in response to Appendix A are fixed for the duration of the project. There shall be no adjustment to the prices provided in this Appendix.

7. All costs associated with the scope of work set forth in this RFT are to be included in this Appendix.

8. Any costs associated with the completion of the required scope of work that are not specifically noted as line items in the charts are to be included in the lump sum pricing.

9. Separate Prices and Alternate Prices must be submitted no later than the Submission Deadline. The remaining pricing forms are to be submitted via email to the administrator within **twenty-four (24) working hours** of the Submission Deadline, which for greater certainty is the date noted as the Supplementary Submission Deadline in the Timetable in Section 5 of the RFP.

Price A – Lump Sum Price for the Work

Proponent Name	

Complete the table below providing a lump sum price for the Work as described in this Request for Proposal. Pricing provided in the table below shall be all inclusive and shall represent the price to execute the work as defined in in this Request for Proposal and associated documentation.

Number of Addendum Received ___ to ___

Cash Allowances noted in the table below will be administered in accordance with the requirements of GC 4.1 of the CCDC 2, 2008 Contract and supplementary conditions.
Cash allowances are to be included in the base bid amount and will be administered based on actual cost. The contractor's base bid amount shall include all OH&P for cash allowances.

Price A - Lump Sum Price for the Work	
Description	Value
Price for the Work	$
Cash Allowances as Directed by CBRE (If Required)	
Cash Allowance 1 Hazardous materials abatement	$ 10,000.00
Cash Allowance 2 DDC Controls	$ 80,000.00
Cash Allowance 3	$
Cash Allowance 4	$
Cash Allowance 5	$
Cash Allowance 6	$
Cash Allowance 7	$
Total Lump Sum Price for the Work	**$**

Signature of Proponent	
Name	
Title	
Date	
Signature of Witness	
Name	
Date	

Price B – Separate Prices

Proponent Name	

Complete the table below providing the separate prices noted below:

Price B - Separate Prices	
Description	Value
	$
	$
	$
	$
	$
	$
	$
	$
	$
	$
	$
	$
	$
	$
	$
	$

Signature of Proponent	
Name	
Title	
Date	

Price C – Alternate Prices

Proponent Name	

Complete the table below providing the alternate prices noted below:

Price C - Alternate Prices		
Description	Add / Credit (+ / -)	Value
		$
		$
		$
		$
		$
		$
		$

Signature of Proponent	
Name	
Title	
Date	

Price D – Unit Prices

Proponent Name	

Complete the table below providing unit prices to be used in the event of changes in the Work.

Description	Unit of Measure	Value
		$
		$
		$
		$
		$
		$
		$
		$
		$
		$
		$

Signature of Proponent	
Name	
Title	
Date	

Price E – Itemized Prices

Proponent Name	

The Itemized Prices requested below are to be **included** in the Price A Lump Sum Price for the Work. The Itemized Prices will not be used to adjust the scope of the work or the Lump Sum Price for the Work.

Complete the table below providing the requested Itemized Prices:

Price E – Itemized Prices	
Description	Value
	$
	$
	$
	$
	$
	$
	$
	$
	$
	$

Signature of Proponent	
Name	
Title	
Date	

Price F – Breakdown of Lump Sum Price for the Work

Proponent Name	

Complete the table below providing a breakdown of the Price A Lump Sum Price for the Work and the included subcontractor for each applicable trade division. The total in the table below must match the total provided for Price A Lump Sum Price for the Work:

Price F - Breakdown of Lump Sum Price for the Work		
Description	Subcontractor	Value
General Requirements		$
Supervision		$
Fabricated Metals		$
Rough Carpentry		$
Finish Carpentry/Millwork		$
Doors, Frames, and Hardware		$
Glazing		$
Interior Architectural Finishes		$
Drywall Framing, Acoustical Ceiling		$
Flooring		$
Painting/Wall Covering		$
Specialties		$
Mechanical/Plumbing		$
HVAC		$
Sprinkler		$
Electrical		$
Communication Cabling		$
Fire Alarm		$
Security		$
Equipment/Appliances		$
		$
		$
Cash Allowances (as noted)		$ 95,000.00
	Total	**$**

Signature of Proponent	
Name	
Title	
Date	

CONFLICT OF INTEREST

SUPPLIER DECLARATION FORM

CBRE has established policies and procedures for reviewing and addressing potential conflicts of interest situations. As part of this process, you, the Supplier, are asked to disclose any and all potential conflicts of interest to CBRE for appropriate review and disposition.

Examples include, without limitation, a CBRE, Province of British Columbia or Ministry employee (hereafter "CBRE or its Client") having an ownership interest in your business, your business being owned by a relative of an employee of CBRE or its Client, or your business sponsoring speaking engagements or other activities with which CBRE or its Client's staff are involved.

Your obligation with regard to the disclosure of conflicts of interest is ongoing, therefore we require that you promptly notify us should you become aware of any potential conflict of interest following the submission of this form.

Supplier Name: _____ Contact Name: _____

Street Address: _____ Phone No.: _____

City, Province, Postal Code: _____ Email: _____

Please select the appropriate statement:

__ I AM NOT aware of any relationship between any employee of Supplier or its subcontractors and an employee of CBRE or its Client which could result in potential personal gain for the employee of CBRE or its Client which could enable the CBRE or its Client employee to influence the Supplier relationship for perceived personal gain.

__I AM aware of a relationship between an employee of Supplier or one of its subcontractors and an employee of CBRE or its Client which could result in potential personal gain for the employee of CBRE or its Client which could enable the CBRE or its Client employee to influence the Supplier relationship for perceived personal gain.

Employee Name: _____

Nature of Relationship: _____

_____

_____

By signing below, you represent and affirm that you have proper authority to act on behalf of the Supplier and that the foregoing statements are true and correct to the best of your knowledge.

_____ _____

Signature Title of Signatory

_____ _____

Printed Name Date

For CBRE Sourcing Dept Use Only

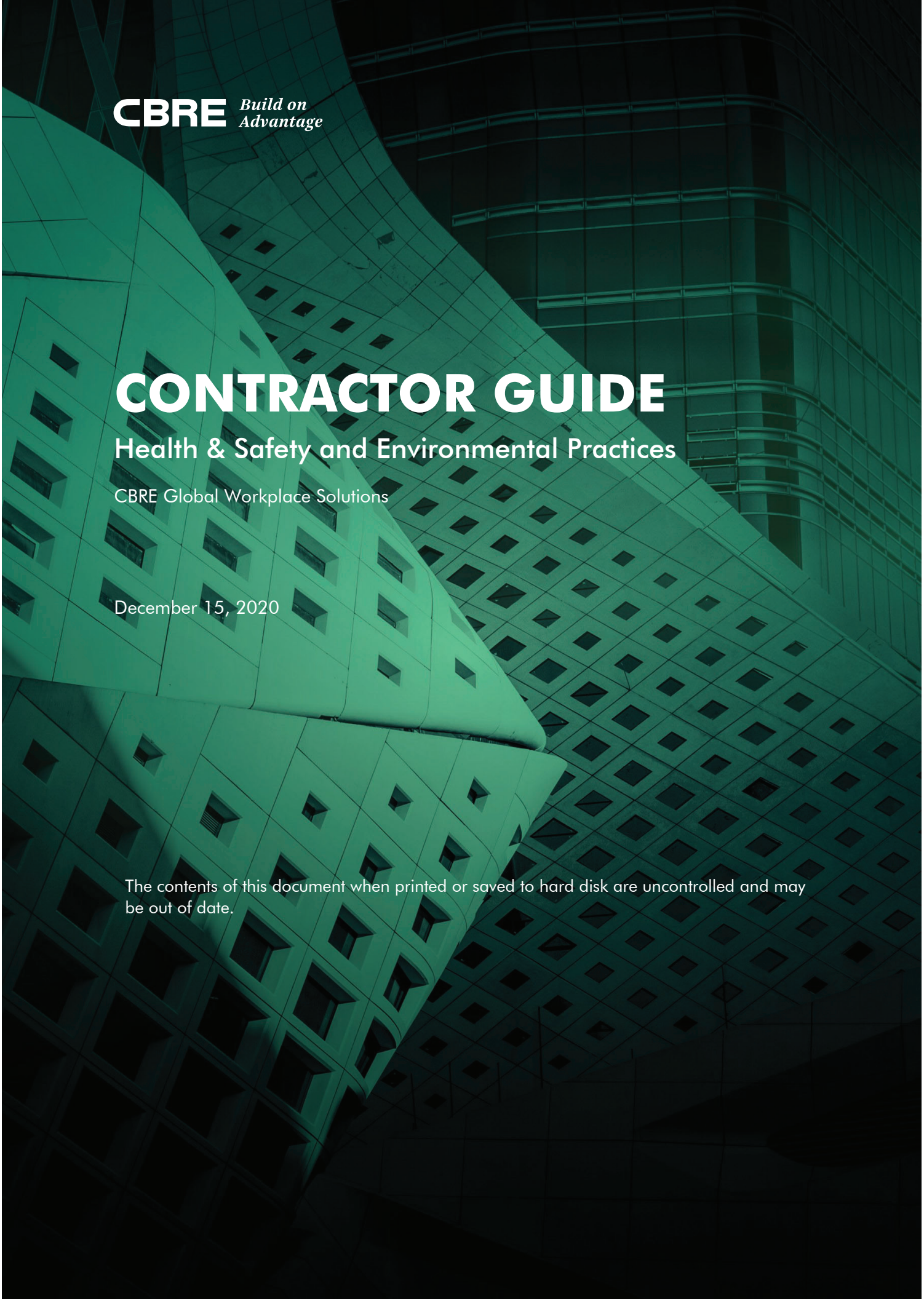
Vendor ID #: _____

Disposition of disclosed potential conflict of interest: _____

_____

_____

Reviewed by: _____ Date: _____



CBRE *Build on Advantage*

CONTRACTOR GUIDE

Health & Safety and Environmental Practices

CBRE Global Workplace Solutions

December 15, 2020

TABLE OF CONTENTS

1.0 INTRODUCTION

Safety of people and the environment is an essential component of every activity of every activity. All retained contractors and their associated sub-contractors will conduct all work in a safe manner and in compliance with all applicable rules, regulations codes and standards. This includes, but is not limited to:

- All applicable federal, provincial and municipal health safety and environmental regulations, by- laws, codes and standards, including building and fire codes;
- CBRE's safety and environmental policies, procedures and programs;
- The contractors' safety and environmental policies, procedures and programs;
- Clients safety and environmental policies, procedures and programs
- Provincial compensation board requirements

This guide has been prepared to ensure the safe completion of work by all retained parties and is applicable to all contractors engaged directly by CBRE and their sub-contractors. This guide is to be included as part of the Terms and Conditions for all vendors, whether on a vendor list or retained directly by CBRE to conduct work.

All contractors will communicate this guide to all employees and sub-contractors and ensure the contents of this guide are fully understood.

Under no circumstances is this guide to overrule the requirements of the federal or provincial Health and Safety Acts, Environmental Protection Acts and associated regulations, or any other applicable laws, regulations and standards. If you have questions concerning the safety or environmental impact of an operation or activity, please contact your employer or your CBRE representative.

All contractors and sub-contractors who fail to comply with this guide and all applicable rules, regulations and standards may be terminated.

Safety of humans and the environment cannot be compromised; safe work is part of your job.

2.0 CBRE HEALTH AND SAFETY POLICY

ACCOUNT: Province of British Columbia, Real Property Division

EFFECTIVE DATE: April 1, 2020

BACKGROUND

CBRE Limited on the Province of British Columbia (BC) Account is committed to the health, safety and the wellbeing of all CBRE employees, contractors, and building occupants and visitors.

We are dedicated to *Safety Before Service*, striving for an accident free work environment, and the ongoing protection of all our employees from injuries or occupational diseases through the implementation of programs, communication, instruction, and training.

POLICY STATEMENT

CBRE commits to the following in our determination to ensure the health, safety and wellbeing of all CBRE employees, contractors and building occupants and visitors:

- Providing safe and healthy working conditions for the prevention of work-related injury and ill health through the implementation of programs, communications, instruction and training.
- Taking all reasonable precautions to ensure the protection of our employees, contractors, and building occupants and visitors.
- Eliminating hazards and reducing Occupational Health & Safety (OH&S) risks.
- Ensuring compliance with all applicable Occupational Health & Safety (OH&S) regulations and other health and safety legislative and/or legal requirements.
- Integrating Health and Safety into all areas of the business.
- Continually improving the Health and Safety Management System.
- Setting annual OH&S objectives that reflect our commitment.
- Consulting and seeking participation from representatives from all workplace stakeholder groups, including workers.
    - Where applicable, Joint Health & Safety Committee worker members will also be consulted regarding health and safety matters.

ACCOUNTABILITIES

The CBRE Province of BC Account will not allow, under any circumstances, any deviations or exceptions to the Health and Safety Management System.

Every person is accountable for ensuring the safety and wellbeing of themselves, the contractors they work with, and building occupants and visitors. This includes the requirement for CBRE employees, contractors, building occupants and visitors to immediately report all unsafe conditions to their direct supervisors or Health and Safety Manager, and to ensure that appropriate corrective action is taken in a timely manner.

The CBRE Province of BC Account Senior Management team is responsible for the implementation of the Health and Safety Management System within their respective lines of business.

All CBRE Province of BC Account directors, managers and supervisors are responsible for demonstrating leadership and commitment in all health and safety matters, and in developing and maintaining a positive health and safety culture.

All CBRE Province of BC Account team members are responsible for:

- Creating and maintaining a safe and healthy work environment through compliance with the OH&S Regulations and Standards.
- Integrating each part of the CBRE Occupational Health & Safety Management System (OH&S MS) into all aspects of operations and culture.

By conforming with the requirements of the ISO 45001:2018, our intent is to deliver industry-leading services while ensuring the health, safety and wellbeing of all CBRE employees, contractors and building occupants and visitors.

Atanu Guha
General Manager, CBRE
Province of BC, Real Property Division Account

3.0 CBRE ENVIRONMENTAL POLICY

ACCOUNT: Province of British Columbia, Real Property Division

EFFECTIVE DATE: November 6, 2020

BACKGROUND

In 2007, CBRE announced our position on environmental sustainability, recognizing the responsibility that comes with our industry leadership position. Since then, we have improved our internal operations, engaged our clients globally to assist them in their sustainable practices, and collaborated with non-governmental organizations in dialog around environmental sustainability.

In 2010, we became the first company in our industry to achieve carbon neutrality in its operations.

Commitment to corporate citizenship and embracing the CBRE Core Values of Respect, Integrity, Service, and Excellence are fundamental goals of CBRE and our worldwide affiliates. These Core Values, combined with our commitment towards sustainability, have shaped our Environmental Policy. CBRE will communicate this policy with all employees, sub-contractors, and any other interested parties.

POLICY STATEMENT

CBRE commits to the following in our determination to increase our environmental performance:

- Implementing environmentally sustainable best practices for our own operations, and assisting our clients to address their environmental concerns, to prevent pollution and protect or improve the natural environment.
- Meet or exceeding all applicable environmental legislation or other required standards.
- Integrating environmental management into all areas of the business.
- Monitoring progress in meeting environmental targets and objectives.
- Continually improving the Environmental Management System.

ACCOUNTABILITIES

All CBRE Province of BC Account team members are responsible for understanding their own environmental impacts and conducting their work in a way to reduce those impacts where possible.

The CBRE Province of BC Account Senior Management Team is responsible for the implementation of environmental programs within their respective Lines of Business.

By conforming with the requirements of the ISO 14001:2015, our intent is to deliver industry-leading services while conserving and restoring the environment where possible.

Atanu Guha
Alliance Director, CBRE
Province of BC, Real Property Division Account

4.0 GENERAL RULES AND REQUIREMENTS

4.1 Contractors' HSE Program

It is CBRE's expectation that all contractors have a formal Health and Safety and/or Environment programs appropriate to the size of the company and the risks of services performed. The Health and Safety program should include but not limited to the following elements:

- Health and safety policy signed by a company executive
- Objectives and targets
- HSE performance metrics
- Hazard identification
- Risk mitigation / control processes in place
- Training matrix and program
- Incident management program
- Return to work program
- Internal audit program
- Management review and continual improvement
- Subcontractor management program

As part of this program, all contractor employees will have received awareness and practical training relevant to the safety or environmental hazards identified and are competent to complete all tasks assigned to them.

All equipment and PPE required to complete the assigned work are to be provided by the contractor. It is the expectation that all employees have been provided personal PPE appropriate to the tasks and have been trained in the proper inspection, maintenance and use of the equipment.

CBRE reserves the right to request all documentation associated with these requirements. Contractors may be terminated for inability to comply.

4.2 Job or Project Specific H&S Plan

Contractors are required to provide a project or job specific H&S plan upon request. The plan must align with the Building H&S Plan (where in place), project specifications and the contract. The contractor is to present and review the project or job specific plan to the CBRE representative to ensure there are no inconsistencies or gaps with the internally conducted job or project risk assessment.

4.3 Reporting of Hazardous Conditions

All contractors are to report immediately to their CBRE representative any hazardous conditions observed. Contractors will not undertake work in the area where the hazardous condition exists.

4.4 Incident Reporting

Contractors are to provide an immediate notification of all incidents to their CBRE representative. A written report should follow within 24 hours. Incidents include the following:

- All injuries requiring attention beyond first aid
- Impact to the building occupants (e.g., evacuation, IT or utility disruption)
- Property damage including third party property
- Release of a contaminant to the natural environment (including releases to a sewer system)
- Harmful activities to flora/fauna at site
- Incidents involving workplace violence or harassment
- Incident requiring notification to a regulatory authority
- Warning letters or orders received by any regulatory authority
- All fires
- Unplanned disturbance of suspected asbestos (see section 3.12.2 Asbestos)
- All significant near misses

Contractors are responsible for providing notification of injury to WorkSafeBC in accordance with their requirements.

CBRE reserves the right to request a copy of the investigation report and of the status any corrective actions.

4.4.1 Non Compliance / Progressive Disciplinary Process

Contractors are responsible for managing their employees and addressing all reported non-compliance concerns. Contractors are responsible to initiate an investigation as well as administer an appropriate disciplinary process for all known incidents.

For all issues regarding non-compliance or non-conformance and infractions, including orders issued by any regulatory body in regard to their work or construction-site, contractors are fully responsible to rectify and correct all non-conformances within the timeframe as issued. Contractors are also to submit a written report detailing all root causes and corrective actions taken to comply with the non-conformances to the CBRE representative for review. The CBRE representative has the discretion to escalate all issues to corporate management.

4.5 First Aid

All contractors are responsible to provide first aid to their employees. It is CBRE's expectation that contractors will provide the personnel, training, kits and equipment

appropriate to the work and number of employees on site, and that all equipment are maintained.

CBRE reserves the right to request the training records for first aiders located on-site.

4.6 Security Clearances and Key Authorization

Contractors are responsible to confirm with the CBRE representative all security clearances required to access the site and to obtain the necessary entry permit and / or key authorization. All authorized keys and/or entry permits are to be returned to the CBRE representative or designate upon leaving site or at the end of the work day unless otherwise directed.

4.7 Site Access and Emergency Procedures

All contractors will report to the person in charge of the site and complete all access requirements (e.g., sign in logs) prior to commencing work, unless otherwise directed. As required, the contractor will provide the names of all employees including their sub-contractors and include details and locations of the work being completed.

All contractors are to review and understand the site emergency and evacuation procedures before starting work on site, including:

- On-site notification procedures
- Location of emergency exists
- Location of emergency, including spill kit, equipment
- Designated assembly area
- Location of nearest hospital

During emergencies and evacuations all employees are to exit the building via the nearest emergency exits. Elevators are not to be used. Contractors are required to report to the designated assembly area at the facility. Leaving the designated assembly area during an emergency is strictly prohibited and may result in removal from site.

4.8 Contractor Conduct

4.8.1 Personal Conduct

Contractors are required to conduct themselves in a respectful manner when working on site. CBRE will not tolerate any contractor using profanity or engaging in horseplay, feats of strength or other behavior that may put themselves or others at risk. Contractors will abide by all rules and policies in place at each facility as well as those set out by the individual building tenant organizations.

In all instances, CBRE expects all contractors to cooperate fully with site personnel. Issues or concerns are to be brought to the attention of the CBRE representative.

4.8.2 Workplace Violence and Harassment

CBRE is committed to maintaining a workplace where employees are free from any form of harassment and violence. All employees are to be treated with respect and dignity. CBRE expects all contractors to adopt the same standard of zero tolerance, and undertaken the prevention and investigation of harassment, violence and all other forms of inappropriate behavior in the workplace. CBRE expects all contractors to take appropriate action to prevent, report and investigate all incidents of this nature and will not tolerate any retaliatory action by any person.

All incidents involving harassment or violent behavior must be brought to the attention of the CBRE representative.

4.8.3 Drugs & Alcohol

Nonprescription drugs and alcoholic beverages are strictly forbidden when conducting work for CBRE. Contractors found in possession of illegal drugs or alcohol will be immediately removed from site and will be subjected to all applicable legal recourses. No person under the influence or possession of drugs or alcohol is to enter or knowingly be permitted to enter a work site.

4.8.4 Prescription Medication

Contractors' employees are to notify their employer if they are required to take a prescription drug and of any restrictions that may affect their ability to perform work safely. CBRE expects contractors to address all such issues and to modify schedules and tasks assigned accordingly.

4.8.5 Smoking

Smoking is prohibited inside all buildings without exception. Smoking is only permitted in designated areas and away from all entrance doorways. Smoking is not permitted when working outdoors, on a roof area or in any underground parking structure.

All provincial and municipal by-laws and site specific smoking rules are enforced at all sites.

4.8.6 Weapons

CBRE prohibits the possession, use or distribution of weapons, firearms and/or explosives (including all concealed handguns regardless of whether the contractor has been issued a license to carry the handgun by any authorized provincial or federal agency) while conducting work at a location for CBRE.

CBRE reserves the right to dispose of any confiscated weapons as appropriate to ensure the safety of all site personnel. CBRE also reserves the right to remove any person found in possession of weapons when on site and contact law enforcement agency as it deems necessary.

It is the contractors' responsibility to ensure none of their employees are in possession of any type of weapon prior commencing work.

4.8.7 Telephone Use

Contractors may not use site telephones unless special arrangements have been made with the CBRE representative or in an emergency situation.

Cellular phones may be used when approved basis by the CBRE representative.

4.8.8 Parking

All vehicles are to be parked in authorized areas only. Parking in restricted areas, fire lanes or roadways is prohibited. Contractors are responsible to make prior arrangements for vehicle and equipment parking with the CBRE representative. Contractor vehicles parked in unauthorized locations will be removed at the owner's expense.

Overnight parking is prohibited, unless specific authorization has been received from the CBRE representative.

CBRE reserves the right to limit the number of contractor vehicles parked on site. . All fees associated

with alternate parking arrangements are the contractor's responsibility.

4.8.9 Driving / Speed Limits

All traffic regulations are strictly enforced at all sites.

Contractors are to abide by all site driving rules. All equipment and vehicle operators must be properly licensed to operate the vehicles or equipment on site.

Contractors may only drive in designated areas and may not drive in areas posted as restricted unless prior authorization is received by the CBRE representative. Contractors may not drive on lawns, sidewalks, or landscaped areas. Any damages due to a violation of this requirement must be repaired at the contractor's expense.

4.8.10 Computer Rooms

Contractors shall not touch any equipment, computers, telephones, or other machinery while performing their work in computer rooms, unless specifically authorized to do so by the CBRE Representative. Only in the case of an extreme emergency, where electrical power to ALL EPO (Emergency Power Off) controlled equipment (computer equipment, air conditioners, etc.) must be stopped, should a contractor hit the red EPO buttons located next to the main entrances/exits of a computer room.

4.8.11 Environmental Impacts

Contracts shall not knowingly or intentionally cause any deleterious impact on the environment while performing work for CBRE. If any real or potential environmental damage is caused the contractor will immediately contact their CBRE Representative and undertake all reasonable activities to mitigate the damage. If the CBRE Representative is not available, the contractor will call the CBRE Operations Centre at 1-877-222-3112.

5.0 HEALTH, SAFETY & ENVIRONMENT RULES AND STANDARDS

Contractors are responsible for the health and safety of people and the environment at the worksite and are to ensure that all employees have been properly trained, have the appropriate personal protection equipment, instructed in their particular task and are knowledgeable of all required health safety and environmental rules, regulations and standards as applicable to the assigned work.

Contractors are expected to actively initiate an effective corrective action process for all non-conformances to ensure measures are taken to avoid any further issues.

Contractors are to ensure that the health, safety and environmental rules as prescribed by the applicable provincial or federal occupational health and safety acts, the environmental protection acts and all other codes, standards and regulations are strictly observed for all work performed.

Contractors are responsible for posting in a conspicuous place on site all the required health and safety documents associated with the work as well as the contractor's contact information, emergency contact information and emergency procedures as required.

5.1 Prime Contractor / Constructor

The role of the Constructor, Prime Contractor or Principal Contractor at a construction project or other workplace includes having total control of all aspects of the work, and particularly as they relate to occupational health and safety. The Constructor, Prime Contractor or Principal Contractor shall provide effective direct supervision of the work so as to ensure conformity to the contract documents, including the requirements of all applicable statutes, regulations, codes, standards or guidelines.

The Constructor, Prime Contractor or Principal Contractor shall have the sole responsibility for oversight of all construction means, methods, techniques, sequences and procedures, occupational health and safety, and the overall coordination of the work.

There may be periods of time when more than one contractor and property or facility management personnel are required to work at the same site, building or area. In these circumstances, all contractors should consult immediately with the CBRE representative to ensure all contractors and property or facility management personnel clearly understand which contractor is undertaking the role of Constructor, Prime Contractor or Principal Contractor, or to collectively coordinate or reschedule some or all of the work to ensure that separation in 'time and space' can be maintained between work activities or projects. If this cannot be achieved, the CBRE representative will designate one contractor to act as Constructor, Prime Contractor or Principal Contractor for all or some of the collective work through contractual assignments or other written agreements.

In all cases of disputes between contractors, the CBRE representative has the final decision to minimize any disruption to the clients and or building users.

British Columbia – OH&S Regulation Part 20: Construction, Excavation and Demolition (20.1-20.3)

All potential contractors who tender to participate as a prime contractor for a CBRE project must comply with WorkSafeBC OH&S Regulations including:

- Mandatory duty under the OH&S Regulation 20 per Sec.118 of the Workers Compensation
  Act must be deemed a "qualified contractor"
- The owner or the designated prime contractor on a construction project must ensure WorkSafeBC receives in writing a notice of project at least 24 hours before work on the project begins at the worksite if;

"(a) the estimated total cost of labour and materials for the work exceeds $100 000;

(b) all or part of the construction project, project, whether a temporary or a permanent aspect of the project, is designed by a professional engineer except for pre-engineered or pre-manufactured building and structural components;

(c) the construction project is a new erection, a major alteration, a structural repair or a demolition of

(i) a building more than 2 storeys or 6 m (20 ft) high,

(ii) a bridge,

(iii) an earth or water retaining structure more than 3 m (10 ft) high, or

(iv) a silo, chimney or other similar structure more than 6 m (20 ft) high;

(d) workers will be working in a cofferdam or in a compressed air environment other than an underground working as defined in section 22.1;

(e) a worker may be required to enter

(i) a trench over 30 m (100 ft) long, or

(ii) an excavation, other than a trench, over 1.2 m (4 ft) deep.

The notice of project must meet the parameters as defined under the WorkSafeBC OH&S Regulation Part 20.2 (2) & if applicable 20.2.1 Hazardous Substances

For non-construction workplaces in British Columbia and where CBRE has contracted with multiple subcontractors for that workplace, CBRE will ensure that the subcontractors comply with the legislated requirements, either directly or through a third party.

For non-construction workplaces in British Columbia where the owner of the workplace or the property manager for the workplace contracts with multiple subcontractors, the owner or the property manager will ensure that the subcontractors comply with the legislated requirements, either directly or through a third party.

5.2 Work Authorization Permit

It is CBRE's expectation that a 'Work Authorization Permit' or equivalent is signed by the CBRE representative prior to undertaking high risk work. Email authorization / signature is acceptable. Permitting requirements may vary at a site level, but at minimum, permits are required for:

- Confined Spaces
- Control of Hazardous Energy
- Disruption to Building Utilities
- Electrical Work
- Hot Work
- Roof Access
- Working in a Critical Environment

For sourced maintenance activities involving high risk activities, an alternative work authorization program may be established. Direction will be provided by the CBRE representative.

5.3 Critical Environment

Additional notifications and procedures are typically required in CBRE or building occupant identified

critical environments, including but not limited to supplementary:

- Permits
- Security / Escorts
- Methods of Procedures

Work in identified critical facilities may not proceed without the explicit authorization of the CBRE Representative.

5.4 Fire Prevention and Protection

Contractors are required to provide all the necessary fire extinguishing equipment for the work being conducted. On site fire extinguishing equipment is for the facility use and may only be used by contractors in the event of an emergency directly related to the project or work assignment.

Prior to the commencement of work, appropriate and suitable extinguishing equipment which will permit the evacuation of the area during a fire must be in place. All equipment is to be certified with appropriate CSA, ULC or NFPA ratings. All fire extinguishers are to have an Underwriters Laboratories of Canada rating, an inspection tag and current inspection date.

If any part of the fire protection system in a facility is to be disabled due to the work being performed, contractors are required to receive authorization from the CBRE representative prior to commencing work, disclosing all details and nature of the work. Contractors are also required to post notices and provide sufficient fire watch for the period of time the system is disabled. The contractor is to provide written notification that the disabled system has been restored to its proper operating requirements at the conclusion of the fire watch. For all fire watch activities, the contractor must provide the CBRE representative with a report detailing the entire watch period and locations affected.

5.5 Working Alone

CBRE expects that all contractors have and enforce their own individual working alone procedures. For sites where no CBRE person is assigned or permanently located, the contractor is to advise the CBRE representative or designated site contact person upon arrival and departure from the site.

5.6 Warning Signs

Contractors are required to follow all posted warning, safety and security signs and barriers are posted.

Contractors are required to provide and post warning signs, barriers, barricades, etc., as appropriate to the work being undertaken and the risk to the building tenants and general public. Contractors are responsible to ensure all warning signs and or tags are clearly legible and in both official languages where required.

All signs posted must meet the requirements of the applicable regulations and be posted in sufficient numbers to provide adequate warning of the hazards associated with the work taking place.

The contractor is responsible to remove all warning signs posted in their work area at the end of the work.

Where signs and barricades do not provide adequate protection, particularly along a road or walkway, flagmen are to be used.

5.7 Mobile Cranes / Heavy Equipment

Contractors are required to receive authorization from the CBRE representative prior to bringing mobile cranes or other heavy equipment on-site. Contractors are to provide all

details as to the type of equipment, where it will be used, and the length of time it will be on site. The contractor is also responsible to secure the area in which the equipment is to be operated and provide and post appropriate warning signs.

If the equipment is to remain on site for the length of the work, all equipment is to be parked in an authorized, designated area which minimizes the impact to the building users and general public. Contractors are responsible to ensure the use and storage of the equipment will not pose a safety risk to either building occupants or general public.

All heavy equipment is to be inspected daily and prior to use.

The contractor is required to have a written procedure in place for the safe operation of equipment around or near any power lines or outdoor electrical equipment. Operation of equipment near power lines shall conform to the minimum distance allowances as per regulatory requirements *"WorkSafeBC OH&S Regulation Part 19: Electrical Safety 19.24.1 /19.24.2*

5.8 Traffic Control

Contractors are responsible to implement traffic control measures in all areas where the work will interfere or delay the normal flow of traffic on site. The contractor is responsible to implement alternate routes of travel as necessary and these routes are to be clearly marked, secured from the work area and easily accessible for all users. Traffic control measures are to be authorized in advance by the CBRE representative and are to minimize disruption to the building users and the general public.

When using a traffic control person (flag person) contractors are responsible to ensure this person is competent and has been given adequate oral and written instructions for the work at hand, is dedicated solely to traffic control and is provided with the appropriate high visibility PPE. Consideration should be given to minimize environmental impacts, including detours through natural areas, vehicle run-off, and potential collisions with fuel or other hazardous chemical storage on site.

5.9 Loading Docks

Regular loading dock areas may be used for loading or unloading provided prior arrangements have been made with the CBRE Representative. When using loading docks, the driver will be responsible to ensure all wheel chocks are put in place to secure the vehicle. Once the loading or unloading of the vehicle is complete, the vehicle is to be removed immediately.

5.10 Storage

The contractor may store material on site with authorization from the CBRE representative. Contractors are responsible to manage the storage areas, including securing against unauthorized access. Storage areas are to be located where there is minimal impact to the building, site tenants or surrounding environment. The storage

of hazardous materials must meet all applicable regulatory requirements for safety and environmental protection. Emergency procedures appropriate to the type, quantity and location the material is being stored are to be in place. Any stored chemicals must abide by section

3.13.10 Hazardous Materials

5.11 Personal Protective Equipment (PPE)

It is the contractors' responsibility for the provision of personal protective equipment for their employees, suitable and appropriate to the work being conducted. Each employee is to have individual equipment; PPE is not to be shared among employees. Contractors must also be able to demonstrate that the employees have been trained in proper inspection, maintenance, and safe use of the PPE.

5.11.1 Footwear

Contractors are to wear approved safety footwear when working on site. All footwear will be at a minimum grade 1 safety toe impact protection and puncture protection signified by the CSA green patch (triangle) on the footwear. Contractors working around or servicing electrical equipment are to wear electric shock resistant footwear, signified by the CSA approved white triangle with the Greek letter omega. It is recommended that all contractors wear slip resistant footwear due to the varying conditions in all workplaces.

5.11.2 Eyewear / Face Protection

Contractors are required to provide their employees with eyewear or face protection appropriate to the nature of the work being conducted. All eyewear and face protection are to meet the CAN/CSA standards.

5.11.3 Hand Protection

Contractors are required to provide their employees with hand protection appropriate to the nature of the work being conducted. All hand protection are to meet CAN/CSA standards.

5.11.4 Head Protection

Contractors are required to provide their employees with head protection appropriate to the nature of the work being conducted. Contractors working in areas of low head room or where overhead work is being conducted are required to wear approved hard hats meeting or exceeding CAN/CSA Standard Z94.1. Head protection is also be required at all sites where a head protection use policy is in place.

5.11.5 High Visibility Clothing

Contractors in areas with vehicular traffic are required to wear high visibility clothing. All persons involved in ground maintenance will be required to wear such clothing during the course of performing their work while on site.

5.11.6 Hearing Protection

Contractors are required to provide their employees with hearing protection appropriate to the nature of the work being conducted. Hearing protection applies to both indoor and outdoor work. Personal Sound Transmission Devices (i.e. iPods, music playing devices) or any other personal devices that may impair hearing are prohibited.

5.11.7 Specialized PPE

Contractors are required to provide their employees with specialized personal protective equipment appropriate to the nature of the work being conducted. The contractor is responsible to train all their employees required to use and wear any specialized PPE.

5.11.8 Personal Fall Arrest / Restraint Equipment

Contractors are required to provide their employees with fall protection appropriate to the nature of the work being conducted. Only CSA approved fall arrest equipment carrying the approved CSA labels are acceptable. All employees required to use Fall Arrest / Restraint equipment must be properly trained in its use.

5.11.9 Respiratory Equipment

Contractors are required to provide their employees with respiratory protection appropriate to the nature of the work and the environmental conditions. Respiratory protection is to be NIOSH approved and meet the applicable Canadian standards. Contractors are required to ensure all employees required to wear a respirator have been fit tested by a certified safety professional and are clean shaven.

5.12 Regulated Substances

Prior to commencing work, contractors are to request from the CBRE representative, information on all regulated substances which may be located within the work area and are to implement the appropriate safety precautions.

5.12.1 Designated Substances

Contractors are responsible for ensuring full compliance with (Chemical Agents & Biological Agents & OH&S Regulation Part 6: Substance Specific Requirements) Contractors are responsible for all medical surveillance and medical records of their employees' exposure to a chemical or biological agent.

5.12.2 Asbestos Containing Materials

Prior to conducting any work on-site, contractors are to request the facility Asbestos Survey Report from the CBRE Site Representative to ensure that known or suspected asbestos containing materials are not unintentionally disturbed during the course of work. Contractors are to stop work and notify the CBRE representative immediately if previously unidentified suspected or known asbestos material is encountered, or if known asbestos-containing materials are identified to be in fair or poor condition.

All work involving planned or possible disturbance of asbestos-containing materials must comply with WorkSafeBC regulations. Authorization is required from the CBRE representative before initiating any work that will involve asbestos and must be conducted in a manner that minimizes impact to the building occupants.

Contractors conducting work involving asbestos are required to have the requisite training and insurance. All asbestos work is to be conducted in accordance with the building requirements, which may include supervision by a qualified hazardous materials consultant and air monitoring. Contractors

are responsible for providing advance written notification to provincial authorities when such notification is required.

The disposal and transport of asbestos waste is to comply with requirements of the applicable federal and provincial environmental protection and transportation of dangerous goods legislation.

5.12.3 Lead

Lead may be present in a number of materials in buildings, including paint, mortar, glazed ceramics, and solder. Contractors are to confirm with the CBRE representative all materials identified as lead containing before conducting work that may disturb the material.

Authorization is required from the CBRE representative before initiating any work that involves disturbance of lead. Any disturbance of lead containing materials is to be conducted using the appropriate lead safety precautions, and are to follow all building specific requirements, which may include supervision by a qualified hazardous materials consultant and air monitoring. Contractors are to notify the CBRE representative immediately, if suspected or known lead material is encountered.

The disposal and transport of lead waste is to comply with requirements of the applicable federal and provincial environmental protection and transportation of dangerous goods legislation.

5.13 Work Area

5.13.1 First Aid / Emergency Equipment

Under no circumstances are first-aid equipment, fire extinguishers, fire blankets, stretchers, eyewash fountains, deluge showers, and other emergency equipment, to be moved, relocated or blocked unless absolutely necessary and alternate equipment is provided in the interim. In all instances authorization from the CBRE representative is required.

Contractors are to provide first aid supplies and ensure the appropriate number of trained first aid responders is located on-site in accordance with applicable provincial regulations.

Contractors are required to provide their own safety equipment appropriate to the work being conducted on-site. All emergency equipment, fire extinguishers, first aid kits, eye wash stations, must meet at a minimum all applicable CSA standards and ULC codes as required. Emergency equipment not meeting the required minimum standard will not be allowed on site.

Contractors are responsible to determine the correct quantity of emergency response equipment to be located on-site and are to ensure that the equipment is replaced as used. In the event that a contractor is required to use emergency equipment, the contractor is obligated to provide the CBRE representative with a complete report detailing the circumstances for the use and corrective actions taken to prevent any further incidents.

5.13.2 Contamination Control

Contractors are required to take all necessary precautions to prevent and control any and all contaminants that may negatively impact the building occupants, equipment, the general public, or the surrounding environment. Contaminants include thermal and noise contamination. Enhanced mitigation measures may be

required if the work is being conducted in areas of sensitivity (e.g., laboratories, location with sensitive equipment, riparian zones, etc.).

Work generating a contaminant is to be scheduled in accordance with best engineering practices and at times that will minimize negative impacts. Contractors shall consultant with the CBRE representative to ensure that work generating a contaminant is performed in compliance with any other site-specific requirements.

Contractors may be required to provide contaminant monitoring. Contractors are to ensure all employees wear the appropriate PPE where exposure to a contaminant is possible.

5.13.3 Hygiene

Arrangements for access to washroom and eating facilities are to be made in advance with the CBRE representative. For work or projects where portable facilities are required, contractors are to verify with the CBRE representative as to where the portable facilities may be located. Contractors are responsible to ensure an adequate number of facilities are provided, properly maintained, within easy access for contractors to use and are adequately supplied with required sanitary items. Contractors are also to verify with the CBRE representative for appropriate rest / eating areas if on site facilities cannot be used.

Contractors are responsible to supply adequate amount of drinking water for employees if potable water is not available at the work area or facility. Any impact to onsite drinking water must be immediately reported to the CBRE Representative and the contractor must undertake all reasonable activities to mitigate the risk. If the CBRE Representative is not available, then the contractor will call the CBRE Operations Centre at 1-877=222-3112.

5.13.4 Housekeeping

Contractors are responsible to ensure the work area is clean and organized at all time. All tools and equipment are to be carefully stored and located so as not to block aisles, doors, fire extinguishers, fire blankets, stretchers, emergency eye wash fountains, emergency safety showers, fixed ladders, stairways, first-aid stations, elevators, etc. Contractor storage areas, if available, will be designated by the CBRE representative and be properly marked. Contractors are responsible to maintain order in the storage areas.

Nails protruding from boards are to be removed or bent over. Foam, scrap lumber, and all other debris are to be kept clear of all work areas.

Contractors are to ensure that no trip hazards exist. This includes any materials or objects protruding from floor surfaces, such as cable conduits etc. Objects protruding from floor surfaces must be made visible by placing an orange safety cone or other visible covering over the object.

Contractors are to obtain the authorization from the CBRE representative for the use and location of a large disposal container.

Combustible scrap, waste materials, and debris are to be removed at regular and frequent intervals, and the removal must be in compliance with any federal or provincial waste management and environmental legislation and in approved containers.

Overhead storage of debris, tools, equipment, etc., is prohibited. No loose material is to be left in the area above suspended ceiling panels. All stacked material will be properly secured to prevent it from collapsing or falling. Material stored outdoors or on a roof top shall be properly secure to prevent it from being blown by high winds.

Carts, tools, materials, and equipment are not to be left unattended in aisles or stairways.

5.13.5 Material Handling

Wherever practical, heavy lifts are to be conducted with mechanical devices. Contractors are to know their physical limitations and approximate weight of materials being lifted. Contractors are encouraged to ask for assistance when the lifting task may be more than can be safely handled and are to use proper lifting techniques to prevent injuries. Wherever possible, dollies, pump trucks, 2-wheel carts and similar devices are to be used.

Piping, conduit, and other materials over 3 meters (10 ft.) long are to be carried by two contractors, each worker supporting one end of the material to be transported.

When transporting piping, conduit, and material under 3 meters (10 feet) in length, the forward end of the material should be raised above head height to reduce the possibility of striking on-coming personnel.

5.13.6 Portable Heaters

Authorization is required from the CBRE representative before any portable heater may be brought on- site. All portable heaters are required to be approved by the Canadian Standards Association, or Underwriter's Laboratory.

Portable heaters are only to be used as a source of supplemental heat and not as the primary heat source, except in an emergency situation. Heaters may not be left unattended and are to be placed a minimum distance of 3 feet from any flammable or combustible materials and observe a minimum overhead clearance of at least 6 feet.

Contractors are to ensure adequate ventilation is present if gas fired heaters are in use and cannot be used in a confined space. Exhaust from gas heaters is to be ducted to the outside environment.

Cylinders for propane heaters are to be placed at minimum of 10 feet from the heater and away from all heat sources. Propane cylinders are to be stored in a secured outdoor location.

For diesel or kerosene fire heaters, the heater unit is to be off and cool to the touch before re-fueling. Fuel is to be stored away from the heater and in a well-ventilated area. Indoor storage is to be in a well- ventilated area or cabinet meeting all fire code requirements.

Heaters are to be placed on a stable level surface to prevent being overturned and away from all travel ways. Heaters are to be periodically inspected to ensure safe operation following the manufacturer's instructions and serviced only by a licensed service technician.

Contractors are responsible to provide the necessary firefighting equipment in the immediate area where the unit is placed.

Heaters are not to be left on overnight.

Failure to observe all safety measures will result in their removal from site.

5.13.7 Combustion Engines

Authorization from the CBRE representative is required prior to bringing combustion engines on-site.

Gasoline, LP gas or other internal combustion engines are not to be operated inside buildings unless approved oxy-catalyst exhaust purifiers are used, the exhaust is piped to an approved exhaust venting system or the exhaust is piped outside the building through a flexible or permanent exhaust hose.

5.13.8 Tarpaulins

All tarpaulins used at site are to be flame resistant and in good condition.

5.13.9 Floor Openings and Utility Holes

Floor openings and manholes are to be guarded by substantial and properly secured barriers, railings, or covering material substantial enough to sustain twice the load of pedestrian or vehicular traffic. In addition, all floor openings are to be clearly marked and identified as such (i.e. open hole below).

Where a danger of falling exists, elevated floor areas are to be provided with guardrails. In addition, toe-boards are to be provided when the possibility of falling objects striking personnel below exists.

Contractors are responsible for replacing any floor opening cover if removed, upon completion of work or if the area is left unattended.

5.13.10 Hazardous Materials

Contractors are required to obtain authorization from the CBRE representative prior to bringing hazardous materials to a work location. Only minimal quantities are to be brought and maintained at site. Contractors are to maintain an updated inventory of hazardous materials on-site; current Material Safety Data Sheets are to be located in proximity to the hazardous materials storage and areas of use and must be accessible to CBRE and emergency response personnel. All emergency contact numbers are to be clearly posted in the storage area.

Contractors are responsible to ensure all hazardous materials are properly handled, stored and disposed of in accordance with all regulatory and code requirements, which includes providing an appropriate spill response plan and maintaining the appropriate emergency equipment on-site

Contractors are to be able to demonstrate that employees have received WHMIS training and are knowledgeable in spill response appropriate to the material at the work location. Any releases or spills that results in a requirement to contact a regulatory authority must be investigated and reported.

In addition, contractors are to be able to demonstrate that employees involved in the transporting of hazardous materials have Transportation of Dangerous Goods training appropriate to their role.

All flammable and combustible liquids must be stored in approved containers or flammable/combustible storage room which meets all code and regulatory requirements. Contractors are to ensure only the minimal amounts of flammable / combustible liquids are stored on site and in a well-ventilated area. All storage areas are to be clearly labeled, with appropriate signs indicating the hazard.

Contractors are responsible to ensure all flammable and combustible liquids in-use are not placed in or around any potential sources of ignition. In addition, a fire extinguisher appropriate for the use is required in the immediate area. When transferring or decanting flammable and combustible liquids, contractors are to ensure all safety precautions are in place including bonding and grounding of the containers.

All compressed gas cylinders are to be stored, transported and used in a secure upright position. When not in use, the protective cap is to be placed on the cylinder

and properly secured. All compressed gas cylinders both spent or full are required to be stored in a secure, clearly marked location, removed from any potential ignition sources, common travel paths and means of egress.

If any real or potential environmental damage is caused the contractor will immediately contact their CBRE Representative and undertake all reasonable activities to mitigate the damage. If the CBRE Representative is not available, the contractor will call the CBRE Operations Centre at 1-877-222-3112.

5.13.11 Solid Waste Management

Contractors are to minimize generation of solid waste created as part of their services and are to participate in all recycling programs available. Contractors are responsible to verify that all waste / recycling are properly handled, stored and removed in accordance with all regulatory and code requirements.

5.13.12 Hazardous Waste Management

Contractors are responsible to manage and dispose of all hazardous waste in accordance with applicable regulatory requirements.

5.13.13 Water

Contractors are to ensure that any waste or contaminants do not enter the sewer or stormwater system. In the event of discharge, immediate notification to the CBRE representative and incident reporting is required, refer to Section 2.4.

Contractors are to receive authorization from the CBRE representative prior to drawing large quantities of water from the facility's water supply and prior to adding substances to the facilities plumbing system (e.g., pouring materials down the drain).

If any real or potential environmental damage is caused the contractor will immediately contact their CBRE Representative and undertake all reasonable activities to mitigate the damage. If the CBRE Representative is not available, the contractor will call the CBRE Operations Centre at 1-877-222-3112.

5.13.14 Energy

CBRE encourages contractors to utilize energy efficient equipment as part of their services. The Contractor is to minimize energy consumption during provision of services and inform and obtain permission from the CBRE representative prior to drawing large quantities of power from the facility.

5.13.15 Halocarbons

Contractors that work on systems that contain halocarbons are required to manage those systems in accordance with applicable legislation. Any time a leak test is conducted a leak test tag, approved by CBRE, must be completed and affixed to the unit. Any time service work is conducted the Halocarbon Service log must be completed. A photo of the completed logbook and (if required) leak test tag must be attached to the online work order.

If any real or potential release of refrigerant exists, regardless of size, then the contractor will immediately contact their CBRE Representative and undertake all reasonable activities to mitigate the release. If the CBRE Representative is not available, the contractor will call the CBRE Operations Centre at 1-877-222-3112.

5.13.16 Fuel Storage Tanks

All work on, near, or involving petroleum storage tanks and/or systems is equipment in accordance with appropriate Provincial or Federal legislation and codes. Contractors working on fuel storage tanks must be qualified to work on fuel storage tanks and/or systems.
Contractors who are working near petroleum storage tanks and/or systems must adhere to safety precautions and follow signage by not smoking at all times. Contractors cannot conduct hot work unless authorized.

If any real or potential release of fuel exists, regardless of amount, then the contractor will immediately contact their CBRE Representative and undertake all reasonable activities to mitigate the release and impacts. If the CBRE Representative is not available, the contractor will call the CBRE Operations Centre at 1-877-222-3112.

5.14 Tools and Equipment

5.14.1 Hand and Power Tools

Contractors are responsible for supplying all tools and equipment necessary for the completion of their work. The use of CBRE or client owned tools and equipment is not permitted under any circumstances. Contractors are required to obtain authorization from the CBRE representative to store tools on-site. Tools maintained on site are to be placed in locked containers or toolboxes at the end of the workday. Tools and other materials are not to be left on stepladders, scaffolds, roofs, or other places where they may be dislodged and fall or where they may create a trip hazard. Appropriate PPE is to be worn at all times to protect the user from injury.

All tools are only to be used for their intended purpose. Hand and power tools are to be maintained in good operating condition and inspected before use. All defective tools are to be tagged and removed from service immediately.

Mushroomed heads on cold chisels, star drills, etc., are unsafe and are not be used. Hammer handles are to be intact. Wrenches are not be overstrained by extending the handle with a pipe or by other means.

Only utility knives equipped with a retractable blade are acceptable for use. Worn or broken blades are not to be discarded in the regular trash containers; contractors are responsible to collect and remove these from site.

Electrical tools are to be either grounded (3-wire), double insulated or used with ground fault circuit interrupter (GFCI) protection. Power tool cords and extension cords are to be inspected regularly and replaced if worn or cracked. All guarding or other safety devices on power tools are never to be removed, tampered with or made ineffective in any way. Prior to changing an attachment or making adjustments to any power operated tool, the tool is to be disconnected from its power source.

A Ground Fault Circuit Interrupter (GFCI) is to be used when operating all electrically powered tools outside or in a wet or damp environment.

Non-sparking tools are a requirement where flammable chemicals are handled or where sparks could create an explosion.

All extension cords are to be utilized such that they do not create a tripping hazard.

If working at height with tools close to the edge, all tools must be tethered so as to prevent falling to area below.

5.14.2 Explosive Actuated Tools

Contractors are to obtain authorization from the CBRE representative prior to bringing and using explosive actuated tools to the work area. All explosive actuated fastening tools are to meet the design requirements of the Canadian Standards Safety Code Z166; if they do not meet these design standards they cannot be used on the premises.

The tools are not to be loaded until ready for immediate use. Contractors are not to carry a loaded tool when walking or travelling on site. Under no circumstances is a loaded tool to be pointed in the direction of another person or used in an explosive or flammable atmosphere. Misfired cartridges are required be placed in a water filled container and removed by the contractor from the site.

Failure to observe all safety rules for the use of these tools will result in the immediate suspension of its use on site.

5.15 Construction

5.15.1 Tenant / Public Protection

Contractors are responsible to ensure all travel ways in close proximity to the work area are adequately protected from all potential hazards, which may include physical barriers, fencing or guardrails.

5.15.2 Breach of Wall

Contractors are responsible for restoring any penetrations that are made in any type of walls as soon as possible to maintain a tight seal around conduit, piping, ductwork, etc.

5.15.3 Excavations and Trenches

Prior to conducting any excavation work, contractors are required to ensure:

- All underground utilities are accurately located and marked,
- All services within the excavated areas are rendered inoperative, locked and tagged out,
- Prevention of unauthorized access,
- All precautions necessary to prevent damage to any utilities in the excavated areas are undertaken,
- All precautions to protect all adjacent structures that may be affected by the excavation area are undertaken, including engaging the services of a professional engineer,
- Daily inspections of the excavations are conducted. If there is evidence of possible cave-ins or slides, or signs of water infiltration, all work in the excavation is to cease until the necessary safeguards have been taken,
- All open holes, trenches are barricaded to prevent unauthorized access,
- Personnel do not enter a trench unless another worker is in close proximity and has easy access to the trench,
- The walls of all trenches are supported or shored and all barriers are in place, as required,
- Ladders or other means of access and egress are located no more than 3 meters (10 ft.) of lateral travel between means of access, and
- All excavated material (soils), rock debris or equipment are effectively stored or retained at least 1 meter (3 feet) from the edge of the excavation to protect employees from falling objects.

Regardless of the depth of the excavation, when heavy equipment is to be operated nearby, the shoring or bracing is required to be able to withstand this extra load.

All excavations and trenches are to be back filled and compacted as soon as practical after work is completed and all associated equipment removed.

5.15.4 Construction / Demolitions

Contractors are responsible to ensure all construction, renovation and demolition work is conducted in accordance with all applicable health, safety and environmental legislation. Minimum safety precautions include, but are not limited to:

- The work area is properly barricaded from unauthorized entry and all warning signs are in place,
- All precautions have been taken to prevent injury to employees, building occupants and the public on-site and in the surrounding area that may result from the demolition work (e.g., flying debris, excessive dusts etc.);
- All precautions have been taken to prevent property damage to adjacent and surrounding properties,
- All utilities have been properly located and shut off and or disconnected before beginning the demolition work,
- All toxic, hazardous, flammable or explosive materials and substances have been removed from the building before the start of the demolition process;
- All documentation permits and registrations are in place; and
- All precautions have been taken to prevent damage to the surrounding environment, and especially environmentally sensitive areas.

5.16 Confined Spaces

Contractors are required to have their own confined space program, including rescue plans. Contractor programs are to be adjusted to any building specific safety requirements.

Contractors are to provide their own safety equipment, including PPE, air monitoring and rescue equipment. All rescue personnel and attendants will be supplied by the contractors.

Contractors are to receive authorization from the CBRE representative prior to entering any confined space. Information to be provided includes the space being entered, the work being carried out and the estimated time frame for completion of work.

5.17 Electrical Work

Contractors are required to have their own electrical safety program. Contractor programs are to be adjusted to any building specific safety requirements.

Contractors are required to receive authorization from the CBRE representative prior to shutting down any building electrical systems, circuits or equipment.

5.18 Control of Hazardous Energy

Contractors are required to have their own control of hazardous energy program. Contractor programs are to be adjusted to any building specific safety requirements.

Contractors are required to receive authorization from the CBRE representative prior to locking / tagging out equipment.

Contractors are responsible to provide their employees with appropriate locks, tags and lock out devices as required. Each employee is to be issued individual locks and tags. Every worker involved in a lockout

/ tagout will place his / her own lock(s) on each piece of equipment as required.

Prior to placing a particular piece of equipment in a zero-energy state, the contractor must review all associated pieces of equipment and isolate all energy sources as required. After placing equipment in zero energy state the contractor is to have a procedure in place to verify all energy sources have been de- energized.

The contractor is required to inform the CBRE representative before re-energizing any equipment. Prior to removing locks and re-energizing, all guards are to be put reinstated and the contractor is to inspect all equipment and work area to ensure it is safe to re-energize the equipment.

At the completion of work, each employee must remove their own locks and tags. Under no circumstances is a person to remove another worker's lock. The CBRE representative must be informed prior to initiating any emergency lock removal procedures. The contractor is responsible to complete a detailed emergency lock removal report and submit a copy to the CBRE representative.

5.19 Hot Work

Contractors are required to receive authorization from the CBRE representative prior to commencing any hot work.

5.19.1 Work Area

Contractors are responsible to inspect the work area prior to commencing hot work and remove or protect with appropriate fire blankets, any flammable / combustible materials in the work area. When welding, screens are required around the work area to protect other personnel in the area from welding flashes.

The use of open flames is strictly prohibited in areas where flammable liquids, gases, or highly combustible materials are stored, handled, or processed.

5.19.2 Ventilation

Ventilation is required for all hot work to reduce the concentration of airborne contaminants in the work zone and to prevent the accumulation of combustible gases and vapors. In areas where mechanical ventilation is required, the contractors are responsible to provide the necessary mechanical ventilation equipment and if required to provide air monitoring during the hot work period.

5.19.3 Fire Watch

Contractors are responsible for providing the required fire watch during the hot work and ensure that a 4-hour fire watch is maintained and all adjacent combustible materials are protected or removed.

5.20 Working at Heights

Contractors are required to receive authorization from the CBRE representative prior to commencing any work at heights.

If working at height is required, it is expected that the contractor will have a "Working at height" program that complies with all regulatory requirements. Hand and power tools used close to edge will be tethered as per section 3.15.1.

5.20.1 Ladders

All ladders must meet or exceed the CSA Standard Z11-12. -Portable Ladders are to be inspected prior to each use and defective ladders are to be tagged and removed from service immediately.

Under no circumstances are contractors permitted to use any CBRE or building occupant owned ladders.

Ladders are to be used for accessing a work area and as a work platform unless other alternate means such as scaffolding or mechanical lifts are not practical due to the work location. Only Fiberglass Reinforce Plastic (FRP) type of ladders will be permitted for use in, near or around any electrical equipment. When climbing ladders, the worker is to maintain a three-point contact and cannot carry any tools. Contractors are advised to use ladders equipped with non-slip footing.

Contractors are responsible for ensuring all contractor ladders are labeled with the contractor's name. Contractors are to obtain authorization from the CBRE representative before storing ladders on-site. All ladders are to be stored in an area that will not cause any disruption to the building tenants or CBRE and are secured from unauthorized use.

5.20.2 Overhead Work

For all overhead work, the area is to be properly barricaded and tagged to prevent access to the work area. The barricaded area is to be large enough to protect those in the immediate area from any potential falling debris or tools. The tag shall indicate the reason for the barricade and a contact name and number.

5.20.3 Roof Work

Contractors are to obtain authorization from the CBRE Representative before entering the roof. Prior to entry to any roof area, all contractor personnel must complete a roof access waiver. Completed and signed forms must be returned to the CBRE representative and will remain on site. The waiver is valid for a period of one year from the date of issue. The roof access waiver is site specific and must be completed for each site where roof access is required.

No person is to enter or remain on a roof unless accompanied by at least one other person to act as a safety watch. Maintenance personnel may do inspections on the roof on their own only when radio contact is continually monitored by the building management or security. An exception to this requirement is work involving a "walk along inspection" where no tools are needed.

During all rooftop operations within 10 feet or 3 meters of the roof edge, the contractor is to have a properly secured safety harness or a safety railing (that meets all legal requirements) along the roof edge.

5.20.4 Scaffolds

The use and construction of scaffolding is to comply with industry practice and all applicable requirements (including the manufacturer's requirement). The erection and dismantling of scaffolds are conducted under the supervision and direction of a qualified (competent) person. Contractors are responsible in selecting the proper type of scaffold dependent on the work and are to inspect the area for all hazards prior to erecting scaffolds. All scaffold types are to be inspected by a competent person before use.

All required ties to the structure are to be installed as soon as the scaffold has been completed to the tie- in area during erection. A safe and unobstructed means of access, such as a walkway, stair, or ladder is to be provided to all scaffold platforms. All planking shall be scaffold grade or equivalent. Platform planking shall be secured to prevent movement.

Guardrails, guardrail screens, toe boards, and outriggers are to be used when required. Anchorage and bracing are to be provided so that scaffolds will be prevented from swaying, tipping, or collapsing. The footing or anchorage for scaffolds is to be sound, rigid, and capable of carrying four times the maximum intended load without settling or displacement. Contractors are responsible to ensure all scaffolds are not loaded in excess of their designed and constructed load limit.

All scaffolds in excess of ten meters in height are required to be designed by a professional engineer setting out the maximum load limits and construction instructions. The engineer or designated competent person will supervise the construction, inspect the scaffold before its use ensuring it is constructed in accordance with the design drawings and provide in writing results of the inspection. Contractors are responsible to maintain the design drawings and written statement on site while the scaffold is in use. The documents are to be available for review upon request.

5.20.5 Suspended Scaffolds / Work Platforms / Boatswain Chairs

All suspended scaffolds, work platforms and boatswain chairs are to be constructed and used in accordance with all applicable regulation and are to be attached to a fixed support or outriggers beam in accordance with the manufacturer's instructions.

All system and equipment components are to be properly installed and inspected prior to use, including:

- Failsafe devices such as rope grabs, secondary safety devices and over speed controls are installed and operational,
- All electrical components for power drive units are properly grounded and secured in place,
- All tiebacks for outrigger beams, parapet clamps and lifelines are properly secured to anchor points capable of supporting 10 times the applied load,
- An adequate numbers of counterweights are securely attached to the outrigger beams. If fiber ropes are used, they are to be protected from premature wear or chaffing and abrasion,

Contractors are to ensure an emergency rescue plan is in place, communicated to all contractors involved before the start of the work and that access to the work area is controlled by adequate warning signs and barricades to prevent any unauthorized access.

5.20.6 Multi-Point Suspended Scaffolds

All multi point suspended scaffolds are required to be designed by a professional engineer using good engineering practices and in compliance with all applicable regulations, standards and codes. A structural engineer is required to inspect the building where the scaffold is to be erected and provide a report ensuring the structural integrity of the building is capable of supporting the scaffold. Contractors are responsible for notifying the applicable provincial ministry before erecting and dismantling the multi-point scaffold.

A professional engineer is required to inspect the scaffold after completion of assembly and prior to use to ensure it complies with the design drawings and provide a written inspection report.

Prior to each daily use the scaffold is to be inspected by a competent worker.

Contractors are to maintain on site copies of all record as required by the applicable regulations.

5.20.7 Mobile Elevating Work Platforms

Contractors are to receive authorization from the CBRE representative before bringing any mobile elevating work platforms on site and must coordinate their use to minimize any disruption to the building tenants and general public who require access to the site.

Contractors are responsible to ensure the elevating work platform selected is appropriate for the work being undertaken, the equipment is only used for its intended purpose, is in safe working order and all required maintenance and inspection tags and documents are in place.

Mobile elevating work platforms are not to be used as a means to gain access to higher elevations, with the intent to exit from the platform. Work undertaken using a mobile elevating work platform is to be performed from inside the unit.

Mobile elevating work platforms are not to be operated in the vicinity of any overhead power lines and only operated on solid ground.

All operators are responsible to ensure the safety of the building tenants and general public when using the equipment and are to place appropriate warning signs and barricades in the work area as required.

Contractors are also responsible to ensure all equipment is stored in an area preventing any unauthorized access.

Contractors are to ensure that appropriate traffic control measures are used as necessary when operating mobile elevated work platform. Refer to Section 3.7

Document Information and Help

Document Owner

Please contact for any questions or assistance with this document.

Ryan Lay | Manager, Environment
Province of BC | CBRE Global Workplace Solutions
C 1 (778) 584 0784
ryan.lay@cbre.com

Mario Angelucci | HS Manager
Province of BC | CBRE Global Workplace Solutions
C 1 (778) 222 0475
Mario.angelucci@cbre.com

Document Control.

This document will be reviewed and updated as required.

Version	Created / Changed By	Approved By	Approval / Review Date	Description of Changes
1.0	Mario Angelucci	Divya Natarajan	April 1, 2020	Creation of document
2.0	Ryan Lay	Lexy Relph	December 10, 2020	1. Template updated 2. Additional Environmental items added 3. H&S and Env Policies added

1. WASTE DIVERSION REQUIREMENTS

1.1 CBRE's target for project generated waste diversion with the Province of British Columbia is 75% for each project. Every project is required to report on waste generated, including projects where no waste is generated.

1.2 All bidders must agree to the following as conditions of bid submission:

.1 Identifying a plan to reduce, reuse, and divert waste generated through all project activities where the availability of such facilities and resources are reasonably available.

.2 Maintain records and utilize the Standardized C&D Waste Form as provided by CBRE.

(i) Projects with greater than 2 tonnes of waste must provide appropriate proof of disposal, recycling, and other methods of diversion such as, but not limited to, Pull Tickets, and Waste Manifests.

(ii) Retain all waste disposal and diversion records for 24 months beyond project closeout.

.3 As part of project closeout documents, submit the Standardized C&D Waste Form with supporting documentation as applicable.

CBRE VOR
VENDOR PERFORMANCE PROGRAM

NOVEMBER 2019

VOR VENDOR PERFORMANCE MANAGEMENT

INTRODUCTION

CBRE Limited Vendor of Record ("VOR") Performance Management, details the criteria, process and methodology of vendor performance. It will be done via progressive methodology inclusive of corrective plans, removal/suspension of zones and up to contract termination.

1. PURPOSE

The purpose is to monitor the performance of Vendors to ensure an open, fair, compliant and competitive process including on budget and on time delivery of quality service to CBRE for its clients.

The objectives are to:

- maintain a list of prequalified vendors with acceptable performance.
- ensure vendor compliance with documentation and processes as requested by CBRE
- encourage continuous Vendor improvement and address shortfalls

Ongoing Vendor performance will be assessed to provide Vendors with feedback to facilitate continuous improvement. As applicable, feedback from CBRE to the Vendor will be given through a written evaluation Vendor Performance Scorecard ("VPS"). Sample in Table 2 herein.

2. EVALUATION OF VENDOR PERFORMANCE

2.1 Vendor Performance Scorecard

The VPS, is the form used for reporting Vendor performance. It is used to ensure an objective assessment of a Vendor's performance, by monitoring and reporting on performance in the delivery of CBRE work order requests and projects.

During the term of a Contract, CBRE will document all incidents of deficient performance and/or infractions by way of surveys, emails, minutes of meetings, notices, warnings, action logs and any other related communications, which may later be used to support a deficient performance review.

Vendors should aim for an "Acceptable" rating and all deficient performance in any or all of the 4 key areas in section 2.2. All scores will be recorded, tracked and will affect vendor's overall rating as detailed in Table 1 and managed as per section 2.3.1.

2.2 Scoring Criteria

CBRE will be reviewing vendor's performance in four (4) key areas as follows:

1) Work Order and Project Surveys
2) Solicitations Participation
3) Procurement Compliance
4) Price Competitiveness

2.2.1 WORK ORDER AND PROJECT SURVEYS

Vendor performance will be managed using the results of surveys issued upon completion of the work via Work Order and on Project close-out.
The surveys will be completed by the appropriate CBRE Facility Manager or Project Manager. Results will be tabulated and measured monthly or as determined by CBRE to address improvement.

The survey will report on (1) Quality of Work performed, (2) Responsiveness, Efficiency and Professionalism, (3) On time completion of the work, (4) Completion of Deficiencies and (5) Vendor's overall performance.
Survey respondents will rate the vendor's performance based on the following scale:

0 = Not satisfied
1 = Partially satisfied
2 = Satisfied

Based on the ratings received for each survey question, the total performance rating for the survey will be translated into scores as follows:

0-4 = Not Satisfied
5-7 = Partially Satisfied
8-9 = Satisfied
10 = Exceed Expectation

Vendors are expected to maintain acceptable ratings/scores as detailed in Table 1. Vendor survey results are weighted at 40% on the overall Scorecard.

2.2.2 SOLICIATION AND PARTICIPATION

Vendors are expected to respond to all solicitations as requested by CBRE. This key area will monitor the number of times a vendor does not respond to and/or provide an explanation for not responding to a request for quote. Vendors are expected to maintain acceptable ratings/scores as detailed in Table 1. Solicitation and Participation is weighted at 15% on the overall Scorecard.

2.2.3 PROCUREMENT COMPLIANCE

Vendors are expected to abide by the rules and instructions of a solicitation by complying with all the requirements including any mandatory requirements, e.g. attendance at mandatory site visits/meetings and any other mandatory requirement as detailed. Vendors are expected to maintain acceptable ratings/scores as detailed in Table 1 Procurement Compliance is weighted at 30% on the overall Scorecard.

2.2.4 PRICE COMPETITIVENESS

Vendor's submitted price will be compared with other prices submitted as part of the same solicitation to determine % deviation from mean price. Vendors are expected to maintain acceptable ratings/scores as detailed in Table1. Price Competitiveness is weighted at 15% on the overall Scorecard.

2.3 Performance Reviews

Performance reviews will be conducted with the vendor/s who have achieved scores of less than 8 or 80% either individually for each work order or Project or in aggregate at any time during the term of the Contract. Vendor Performance Methodology is detailed below.

Strategic Sourcing will share the results of the performance review with the Vendor for discussion and development of an acceptable corrective plan. Vendors will be given 7 days to correct or develop a corrective plan to address/resolve the issue. All plans submitted by the Vendors will be reviewed by CBRE for consensus. If no plan is received within the allotted time frame, CBRE may suspend the vendor from that Zone/s for a defined period of time as detailed below or terminate Vendor contract.

VOR VENDOR PERFORMANCE MANAGEMENT

2.3.1 Vendor Performance Methodology – Table 1

Vendor receives:
4 consecutive/aggregate performance failure scores over a 12 month period in one or multiple criteria, will be managed as highlighted below in YELLOW:
1st occurrence -meeting with an acceptable action plan;
2nd occurrence - warning with an acceptable action plan;
3rd occurrence- suspension for a minimum of 6 months and
4th occurrence- removal/termination from that zone/s and or contract.

Vendor receives:
3 consecutive/aggregate performance failure scores over a 12 month period in one or multiple criteria, will be managed as highlighted below in RED:
1st. occurrence - warning with an acceptable action plan;
2nd. occurrence- suspension for a minimum of 6 months and
3rd. occurrence- removal/termination from that zone/s and or contract.

Vendors achieving a GREEN status will continue to participate in the VOR program.

Table 1 – VENDOR PERFORMANCE METHODOLOGY CHART

Vendor Performance Methodology				
	Rating			
Performance Survey Rating 40 %	0-4	5-7	8-9	10
	Consective 3X or in aggreate within 12 months = Termination	Consective 4X or in aggreate within 12 months = Termination	Acceptable	
Solicitation and Participation 15%	0-50%	51-75%	76-99%	100%
	Consective 3X or in aggreate within 12 months = Termination	Consective 4X or in aggreate within 12 months = Termination	Acceptable	
Procurement Compliance 30%	0%	100%		
	Consective 3X or in aggreate within 12 months = Termination	Acceptable		
Price Competitiveness 15%	51+	16-50	0-15%	
	Consective 3X or in aggreate within 12 months = Termination	Consective 4X or in aggreate within 12 months = Termination	Acceptable	

Table 2 – SAMPLE VENDOR PERFORMANCE SCORECARD

VOR VENDOR PERFORMANCE MANAGEMENT

SAMPLE VENDOR PERFORMANCE SCORECARD

Vendor Name	Test Vendor A

Reporting Term	Start Date	4/1/2013
	End Date	3/31/2014

Regions Served	
Central - A	
Central - B	Y
Central - C	
East - A	
East - B	
North - A	Y
North - B	
South - A	
South - B	
South - C	Y
South - D	

Vendor Performance Scores			
	Vendor Survey	40%	99.0%
	Solicitation & Participation	15%	70.0%
	Price Competitiveness	30%	50.1%
	Procurement Compliance	15%	100.0%
	Vendor Total	100%	80.1%
	Total Project Spend ($)	$ 500,000.00	

Vendor Survey		(0.0% - 40.0%) – Not Satisfied	
		40.1% - 70.0%) – Partially Satisfie	
		(70.1% - 99.9%) – Satisfied	99.0%
		(100%) – Exceed Expectations	

Solicitation Participation		(0.0% - 50.0%) – Not Satisfied	
		(50.1% - 75.0%) – Partially Satisfied	70.0%
		(75.1% - 99.9%) – Satisfied	
		(100%) – Exceed Expectations	

Price Competitiveness		(50.1% - 100%) – Not Satisfied	50.1%
		15.1% - 50.0%) – Partially Satisfie	
		(0.0% - 15.0%) – Satisfied	

Procurement Compliance		(0.0% - 99.9%) – Not Satisfied	
		(100%) – Satisfied	100.0%

Canada
CBRE – RPD-PJM
PO Box 304
Bill to ID 223
135 West Beaver Creek Richmond Hill, ON L4B 4R5

To help ensure timely payment of invoices, the following guidelines have been compiled for your reference. Additionally, CBRE requires every vendor to invoice on a monthly basis, usually the first day of the month after the services have been provided, or within 5 business days of the completion of the work or services. All invoices submitted must meet the following requirements:

1. KPO Number
2. Kahua Project
3. Contract reference and CBRE contact name
4. All invoices must be billed to CBRE or c/o CBRE
5. The service location name and address
6. The supplier's remit to name and address
7. The supplier's tax registration number if applicable
8. Tax must appear as a separate line item on the invoice
9. An invoice date
10. A unique invoice number
11. Project description of goods and / or services received
12. Total invoice amount
13. The date the service was performed (start and stop dates)
14. The invoice must be an original
15. The document submitted for payment must be an invoice; not a statement
16. The invoice must not be altered from its original state
17. Invoices requiring back up documentation must be received with all the supporting documentation
18. A separate invoice is required for each purchase order line number

If submitting invoices via Email Submission the below guidelines additionally apply:

1. Invoice submissions should be directed to GWSPOInvoiceProcessing@cbre.com
2. Subject line of email must reflect Client Name; Country; Number of invoices (Client name, Country and number of invoices should be separated by a semicolon - example: Client ABC; CA; 3)
3. Only PDF attachments are acceptable; each attachment should contain only one invoice
4. PDF attachments must be less than or equal to 10MB in total
5. PDF attachments should not be password protected
6. No ZIP or any other compression should be done to the attachments
7. Body of the email should not contain instructions

Invoices not adhering to the requested format will not be accepted and will result in delays in payment.

Schedule B

Province of British Columbia

Required Flow Down Provisions

I. All provisions of this Schedule are intended to supplement the provisions covering the same subject matter set forth in the Agreement, if any, to the extent not in conflict with such provisions. Notwithstanding, any language to the contrary contained in the Agreement, in the event of a conflict between the terms of this Schedule with those terms covering the same subject matter in the body of the Agreement, the terms of this Schedule shall prevail. For purposes of this Schedule the following shall be applicable: the term "Services" shall mean "Work", the term "Service Provider" shall mean "Contractor", the term "Services Worker" shall mean "Contractor Personnel"; and the term "Province" shall mean "Client".

1. DEFINITIONS

Capitalized terms used and not otherwise defined in this Schedule will have the meaning set out in the Agreement. For purposes of this Schedule, unless the context otherwise requires, the following words and terms will have the following meanings:

(a) **"Approved"** or **"Approval"** means, with respect to any document, budget or action to be taken, that such document, budget or action has or requires the prior written approval of an authorized representative of the Province.

(b) "**Facilities**" means the facilities used in providing the Services, including those housing Systems (including Systems awaiting disposal) or Confidential Information;

(c) "**Information Incident**" means an unwanted or unexpected event or series of events that threaten privacy or security of Confidential Information, including its unauthorized access, collection, use, disclosure, alteration, storage or disposal, whether or not in record form and whether accidental or deliberate;

(d) "**PIA**" has the meaning set out in Section 8(b);

(e) "**Security Event Logs**" means any event, notification or alert that a device, Systems or software is technically capable of producing and is configured to produce in relation to its status, such as a notification of configuration change or notification of log-on/log-off events (also referred to as infrastructure event logs); or any event, notification or alert that a device, Systems or software is technically capable of producing and is configured to produce in relation to its function and activities, such as data/traffic/sessions routed, transmitted, blocked or permitted (also referred to as activity/function event logs). Security Event Logs are not limited to security devices, but are applicable to all devices, Systems and software that are technically capable of producing and are configured to produce event logs that can be used in security investigations, auditing and monitoring. Examples of Systems that can produce security event logs are, but not limited to: routers, switches, content filtering, network traffic flow, network firewalls, intrusion prevention systems, servers, applications, databases, operating systems, virtualization platform, application firewalls, authentication services, directory services, DHCP, DNS, and hardware platforms. Security Event Logs are event logs that can be used in security investigations, auditing or monitoring and can give rise to a security incident or Information Incident;

(f) "**Sensitive Information**" means, whether or not in record form:

(i) Personal Information;

(ii) Confidential Information marked or identified when disclosed or entrusted in the custody of Service Provider as "Confidential", "High Sensitivity", "Cabinet Confidential", "Sensitive Information" or the like; and

(iii) other Confidential Information (if any) specified in Appendix 2;

(g) "**Service Provider's Systems**" includes Systems of third parties that Service Provider authorizes its Services Workers to use in providing the Services (for example, the portable computing device of a Services Worker employed by Service Provider who is authorized to use that device pursuant to Service Provider's work at home or bring your own device to work policy or a data storage service used by Service Provider to back-up data);

(h) "**Services Worker**" means an individual involved in providing the Services for or on behalf of Service Provider, including:

(i) a subcontractor if an individual; or

(ii) an employee or volunteer of Service Provider or of a subcontractor (including a Service Provider Personnel);

(i) "**Standing Access**" means administrators have ongoing access to anything that needs elevated privileges, such that not having Standing Access means that administrators do not have ongoing access to anything that needs elevated privileges and must seek permission to perform certain tasks, and when permission is granted, it is for a limited period and with just-enough access as required to perform the applicable Services;

(j) "**STRA**" has the meaning set out in Section 8(b); and

(k) "**Systems**" means the equipment or interconnected systems or subsystems of equipment, including software, hardware and networks, used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, emission, transmission or reception of:

(i) Confidential Information; or

(ii) information, whether or not in record form, used in providing the Services.

2. SCHEDULE CONTAINS ADDITIONAL OBLIGATIONS

The obligations in this Schedule are in addition to other obligations in this Agreement relating to security (if any), including in the Privacy Protection Schedule.

3. SERVICES WORKER CONFIDENTIALITY AGREEMENTS

Service Provider must not permit a Services Worker who is an employee or volunteer of Service Provider to have access to either Confidential Information through Systems supplied by the Services Worker or Sensitive Information unless the Services Worker is contractually bound to Service Provider in writing to keep that information confidential on terms no less protective than applicable to Service Provider under this Agreement.

4. SERVICES WORKER SECURITY SCREENING

In addition to and without limiting any other requirements for security screening set out in this Agreement, Service Provider may only permit a Services Worker who is an employee, volunteer, Subcontractor, Supplier or Managed Supplier of Service Provider to have access to Sensitive Information, the Province's Systems or, subject to applicable laws and any express exception in this Agreement, otherwise be involved in providing the Services if, after having subjected the Services Worker to Service Provider's personnel security screening requirements, which must be no less stringent than the requirements of the Agreement and any additional security requirements Service Provider may consider appropriate, Service Provider is satisfied that the Services Worker does not constitute an unreasonable security risk. Subject to applicable laws, Service Provider must retain records of its compliance with the security screening requirements of the Agreement. If Service Provider is an individual, the Province may subject Service Provider to the screening requirements of the Agreement.

5. SERVICES WORKER INFORMATION SECURITY TRAINING

(a) Service Provider is responsible for ensuring Services Workers are aware of the requirements of the *Freedom of Information and Protection of Privacy Act* as it relates to this Agreement and any other enactment in effect from time to time relating to handling information.

(b) Service Provider must ensure that each Services Worker who will provide services under this Agreement that involve the access to or entry of data into, or other use of, the Service Provider IMS will complete a security training course delivered by Service Provider prior to that person providing those services and Service Provider must obtain Approval of the Province for the security training content of that course.

(c) Without limiting the foregoing, the Province may require particular Services Workers to complete any relevant information security awareness, education and training provided by the Province online or otherwise before those Services Workers may provide specific Services or receive or access particular Confidential Information or particular Systems or Facilities of the Province and may require Service Provider to keep records tracking such training.

For greater certainty, the foregoing training obligations would not apply to an IaaS or PaaS subcontractor that does not have access to Sensitive Information.

6. ACCESS CONTROLS

Service Provider must apply security controls to:

(a) limit access to Service Provider Facilities where practicable and Service Provider's Systems to those persons authorized by Service Provider to have that access and for the purposes they are authorized to perform Service Provider's obligations under this Agreement, which security control must include measures to verify the identity of those persons and to revoke access when conditions for authorization cease;

(b) limit access to records containing Sensitive Information to those Services Workers authorized by Service Provider to have that access and for the purposes they are authorized to perform Service Provider's obligations under this Agreement, which must include measures to verify the identity of those Services Workers and to revoke access when conditions for the Services Worker's authorization cease; and

(c) limit the performance of all maintenance on Service Provider's Systems where a plausible risk exists that records containing Sensitive Information could be accessed by the performers of maintenance, despite Service Provider's efforts to comply with paragraph (b), to either

authorized Services Workers or, if those records cannot be removed first, other persons who are bound by confidentiality agreements and meet security screening requirements that in both cases are no less protective than the confidentiality and security screening requirements of this Agreement.

In all cases, Service Provider must ensure that only Service Provider Resources that require access to Sensitive Information for Service Provider to perform its obligations under this Agreement have access to Sensitive Information and only to the extent and for the time required for Service Provider to perform its obligations under this Agreement.

7. ACCESS AUDIT LOGS

(a) Service Provider must keep in accordance with Sections 7(b) and 7(c) detailed records logging and monitoring accesses to records containing Sensitive Information transported or stored on Service Provider's Systems, except as this Agreement or the Province may instruct otherwise in writing.

(b) The records described in Section 7(a) must include the following details for each event when appropriate for the technology:

(i) Services Worker identification;

(ii) date, time and details of event;

(iii) subject matter accessed; and

(iv) details of unauthorized access.

(c) Service Provider must keep and protect the records described in Section 7(a) from unauthorized access, alteration or destruction for no less than two years after the end of the calendar year ending December 31st in which the records are created unless the Province agrees in writing to a different period. This includes applying security controls to prevent individuals from being able to alter, erase or deactivate records of their own access.

8. SERVICE PROVIDER'S SYSTEMS AND FACILITIES PROTECTION CONTROLS

(a) Service Provider must apply security controls to protect Service Provider's Systems and Service Provider's Facilities from loss, damage or other occurrence, including from fire and environmental hazards and power interruptions, which may result in them being unavailable when required to provide the Services.

(b) If this Agreement limits the processing, transporting or storing of any records containing Confidential Information to particular Service Provider's Systems or Service Provider's Facilities or their specified location or Services carried on them, Service Provider must, before it makes any change to those Systems or Facilities or Services carried on them that risks reducing the security of those records or to their location to different Systems or Facilities, obtain the Province's written agreement or confirmation that a security threat and risk assessment ("**STRA**") or privacy impact assessment ("**PIA**") or both do not need to be performed or updated. Before agreeing, the Province may require Service Provider, at Service Provider's expense, to:

(i) perform or update, or assist the Province or a mutually acceptable third party in performing or updating, a STRA or PIA, or both, in accordance with Province policies, standards, procedures and guidelines, for review by the Province; and

(ii) submit a plan and remediate or otherwise address any security threats or risks or privacy impacts of concern to the Province identified in the STRA or PIA within a reasonable time.

9. INTEGRITY AND AVAILABILITY OF RECORDS

(a) Service Provider must apply security controls to maintain the integrity and availability of records containing Confidential Information or other information under the Province's control while possessed, accessed or processed by Service Provider. This includes controls to protect such records on Service Provider's Systems from malicious code (including viruses, disabling or damaging codes, trap doors, listening devices, computer worms and Trojan Horses), including as appropriate:

(i) ensuring regularly updated software designed to scan for, detect and provide protection from malicious code is installed with real-time scanning and periodic scanning of all discs enabled;

(ii) maintaining and following business continuity plans to recover from malicious code incidents;

(iii) scanning backup media prior to restoration so that malicious code is not introduced or re-introduced into such Systems; and

(iv) installing critical security patches and updates to all installed software.

(b) For Section 9(a), maintaining the integrity of Confidential Information means that, except as this Agreement or the Province may instruct otherwise, the Confidential Information has:

(i) remained as accurate and complete as when it was obtained or accessed by Service Provider; and

(ii) not been altered in any material respect.

10. ADDITIONAL SECURITY CONTROLS FOR SENSITIVE INFORMATION

Service Provider must apply security controls to:

(a) ensure that records (including backup copies) containing Sensitive Information in transit or stored on the Systems or Service Provider's Systems (including portable computing and storage devices) are secured (in accordance with this Schedule) and encrypted in accordance with the Province's "Cryptographic Standards for Information Protection" (as may be accessed, as of the Effective Date, from the website of the Office of the Chief Information Officer at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/im-it-standards), except as this Agreement may specify other cryptographic standards;

(b) protect and limit access to Service Provider's Systems that will transport or store Sensitive Information through the following means when appropriate for the technology by:

(i) segregating or partitioning Systems to separate and restrict access to Sensitive Information from other records (for example, storing Sensitive Information on a computer or server in a separate, password-protected, encrypted virtual disk or folder);

(ii) storing and transporting portable storage devices safely;

(iii) protecting the Systems with a physical locking, restraint or security mechanism;

(iv) ensuring network perimeters and network traffic control points are established or firewalls are installed and enabled;

(v) having appropriate log-in procedures to the Systems and Sensitive Information stored on the Systems, such as:

(A) requiring user identifiers that are unique and personal for log-in;

(B) requiring complex passwords or personal identification numbers (PINs) that are not shared, default or blank and that require changing at predetermined intervals and are encrypted (not displayed) when entered, biometric accesses, keys, smart cards or other logical or physical access controls or combinations of them;

(C) applying locking screen-savers and session time-out mechanisms;

(D) applying limits on unsuccessful attempts to log-in; and

(E) logging unauthorized changes to system security settings and controls that may enable unauthorized access or tampering;

(vi) disabling unneeded ports, protocols and services; and

(vii) performing any remote management in a secure manner, using encrypted communication channels and adequate access controls; and

(c) ensure records (including backup copies) containing Sensitive Information are not disclosed, accessed from, or stored (including on any Services Worker's portable computing device or third party data storage service) outside Canada without the Province's prior written consent, except as may be in a written direction under the Privacy Protection Schedule with respect to Personal Information or, with respect to non-Personal Information as permitted under Section 23.

11. DOCUMENTATION OF SECURITY CONTROLS, INCLUDING CHANGES

(a) Unless this Agreement specifies otherwise, Service Provider must keep detailed records documenting, and logging any changes to, security controls to support compliance with Sections 6, 8(a), 9(a) and 10.

(b) Service Provider's security control documentation and records required to support compliance with this Schedule, including the records described in Sections 4, 5, 7(a) and 11(a), which may be subject to privacy protection laws governing the private sector, but excluding the log described in Section 16(b), are or are deemed to be the sole property of Service Provider and under Service Provider control.

12. PROVINCE'S SYSTEMS AND FACILITIES

(a) If the Province makes available any of the Province's Facilities or Systems for use in providing any Services, Service Provider must comply with:

(i) Section 12.3.1 (Appropriate Use of Government Resources) of the Province's "Core Policy and Procedures Manual", Chapter 12 (Information Management and Information Technology Management) as may be accessed from the website of the Office of the Comptroller General (which, as of the Effective Date, may be accessed through https://www2.gov.bc.ca/gov/content/governments/organizational-structure/ministries-organizations/central-government-agencies/office-of-the-comptroller-general) as it relates to Province's Systems; and

(ii) other policies, standards and procedures provided by the Province, if any, on acceptable use, protection of, and access to, such Province Facilities or Systems,

in addition to other applicable provisions of this Agreement and only permit its authorized Services Workers who have been instructed to comply with such policies, standards, procedures and provisions to have such access.

(b) The Province has the right to:

(i) not make the Province's Facilities or Systems available before Service Provider or Services Worker or both agree to a form of agreement acceptable to the Province on acceptable use, protection of, and access to, such Facilities or Systems;

(ii) not permit particular Systems to connect to the Province's Systems until satisfied with the security controls to be applied;

(iii) keep access and other audit logs and monitor and analyze use of the Province's Facilities and Systems to verify compliance, investigate suspected or actual breaches or Information Incidents and protect the Province's assets, including records, in compliance with laws, including the *Freedom of Information and Protection of Privacy Act* and *Information Management Act*, and the Province's policies; and

(iv) limit or revoke access, in addition to any other rights the Province may have;

provided that, to the extent that the exercise of any of the foregoing rights amount to a Change of the obligations of Service Provider or otherwise imposes costs upon Service Provider, the Parties will meet to discuss whether that impact can be avoided and, if not, that impact will be considered a change under Section 19(b) and will be addressed in accordance with that Section and Section 19(c).

13. NOTICE OF DEMANDS FOR DISCLOSURE

If, after complying with any applicable obligations under this Agreement relating to responding to requests for Personal Information, other Province Information or Province IP, Service Provider is still required to produce, provide access to or otherwise disclose any Sensitive Information pursuant to any enactment or any subpoena, warrant, order, demand or other request from a court, government agency or other legal authority, Service Provider must immediately notify and provide reasonable assistance to the Province so the Province may seek a protective order or other remedy to prevent or limit the disclosure.

14. NOTICE OF INFORMATION INCIDENTS

In addition to any requirement imposed under the *Freedom of Information and Protection of Privacy Act* or other law, if, during or after the Term, Service Provider discovers a suspected or actual Information Incident, Service Provider must:

(a) immediately report the particulars of the Information Incident to, and follow the instructions of, the Province, confirming any oral report with a notice in writing to the Province as soon as reasonably practicable (if unable to contact the Province's Contract Representative or other designated contact for this Agreement, follow the procedure for reporting and managing information incidents on the website of the Office of the Chief Information Officer, which, as of the Effective Date, is located at https://www2.gov.bc.ca/gov/content/governments/services-for-government/information-management-technology/information-security/information-incidents);

(b) make every reasonable effort to recover the Confidential Information or records containing Confidential Information if appropriate in the circumstances and contain the Information Incident, following such instructions as the Province may give.

15. REVIEW OF INFORMATION INCIDENTS AND INVESTIGATIONS SUPPORT

(a) The Province may review any Information Incident (whether or not reported under Section 14) and, if requested, Service Provider must participate in that review and follow any instructions for remediation and prevention to the extent reasonably practicable.

(b) In connection with the occurrence of an Information Incident, the Province will be entitled to conduct, or have an Other Service Provider conduct on its behalf, vulnerability scanning and any other reasonable security testing with respect to the servers and systems of Service Provider (including the Service Provider IMS) to verify Service Provider's correction or sufficient remediation of deficiencies that contributed to the Information Incident. Service Provider will support the Province or any Other Service Provider in performing any such testing.

(c) Service Provider must:

(i) provide adequate investigative support to the Province at the Province's request to enable the Province to conduct its own security investigations into Information Incidents;

(ii) conduct a security investigation in the case of incidents, breaches or compromises and collect evidence, undertake forensic activities and any other actions needed to investigate an incident, breach or compromise;

(iii) provide the Province with a sanitized version of the investigation report and, upon the Province's request, provide the Province with the supporting sanitized logs in conjunction with such investigation report as validation/confirmation of the investigation;

(iv) maintain chain of custody in all security investigations it undertakes;

(v) take appropriate actions to remediate the incident, breach or compromise;

(vi) provide support to the Province in conjunction with the Province's own security investigations into incidents, breaches or compromises affecting the Province's tenancy or information;

(vii) ensure that Service Provider works with and supports the Province if assistance is needed by the Province in legal proceedings in connection with security investigations; and

(viii) ensure all information provided by Service Provider to the Province under this Section 15 is reliable, forensic quality information (including by ensuring the information required for an investigation is collected in a manner that is forensically adequate to support any required legal action) and provided to the Province in a timely manner.

If Service Provider is not in breach of its obligations under this Agreement and the Province requires Service Provider to expend more than a reasonable level of effort to comply with the foregoing, the Province will reimburse Service Provider for the reasonable costs Service Provider incurs in expending effort that is beyond reasonable to comply with the foregoing provided such costs are pre-approved by the Province; such costs including, if applicable, out of pocket costs and reasonable time charges based on Good Industry Practice.

16. RETENTION, DESTRUCTION AND DELIVERY OF RECORDS

(a) Subject to written instruction by the Province to retain for a different period or deliver any records and without limiting any applicable requirements set forth in this Agreement including Article 10 of the main body of this Agreement and Schedule A (Services), Service Provider must retain records in Service Provider's possession that contain Confidential Information until their delivery or disposal as provided in this Agreement. Except as this Agreement or the Province may instruct otherwise:

(i) backup, transient and extra copies of records (including configuration data) that contain Confidential Information must be securely destroyed when no longer needed to perform this Agreement;

(ii) records that contain Confidential Information, other than those destroyed in accordance with paragraph (i), must be securely delivered to the Province when no longer needed to perform this Agreement; and

(iii) if, despite the delivery or disposal of electronic records of Sensitive Information in accordance with this Section, any Sensitive Information remains on the storage media used, the storage media must be securely destroyed.

(b) Service Provider must keep records logging the dates, particulars, format and means of the delivery or disposal of records that contain Confidential Information and deliver any such log records on request from the Province.

17. ADDITIONAL SECURITY TERMS AND CONDITIONS

(a) Service Provider must comply with the additional terms and conditions in Appendix 2. If a provision in Appendix 3 is only applicable to certain types of cloud services, the general provisions in Appendix 2 with respect to the same subject matter do not apply to the other types of cloud services.

(b) Without limiting Service Provider's other obligations under this Agreement, including Sections 11 and 19 through 22 of the main body of this Schedule, if any of Service Provider's Systems do or will utilize, consist of or depend in any way on any cloud service, such as Infrastructure as a Service, Platform as a Service, and Software as a Service (each as defined in Appendix 3), Service Provider must comply with the additional terms and conditions in Appendix 3 with respect to such cloud service. Where any requirement in Appendix 3 conflicts with the main body of this Schedule or any other Appendix to it with respect to a cloud service, the requirement in Appendix 3 will prevail with respect to the cloud service to the extent of such conflict in accordance with Section 34(c).

18. INSPECTION

In addition to any other rights of inspection the Province may have under this Agreement or under statute, the Province has the rights, at any reasonable time and on reasonable notice to Service Provider, to:

(a) request Service Provider to verify compliance with this Schedule to keep security control documentation or records to support compliance; and

(b) enter on Service Provider's premises to inspect, in a manner agreed to by the Parties, and, at the Province's discretion with respect to subsections (i) and (iii), copy:

(i) any records in the possession of Service Provider containing Confidential Information of the Province or other records under Province control;

(ii) any of Service Provider's policies, information management practices or security control documentation required to support compliance with this Schedule relevant to and for the purpose of determining Service Provider's compliance with this Schedule and any other information management requirements under this Agreement;

(iii) any of Service Provider's records which are otherwise required to be provided in accordance with this Agreement and which are required to support compliance with this Agreement relevant to and for the purpose of determining Service Provider's compliance with this Schedule and any other information management requirements under this Agreement, and Service Provider must permit, and provide reasonable assistance to, the Province to exercise the Province's rights under this Section, including providing excerpts of policies to the Provincial auditors (internal or external) and/or a Province designated personnel as evidence to support findings as part of a Province audit, provided such excerpts are held in strict confidence. If any non-compliance or deficiency is found, the Province may (in addition to any other rights it may have) require Service Provider, at Service Provider's expense, to develop and implement a corrective action plan within a reasonable time. If requested by the Province, Service Provider will make documentation referenced in subsection (ii) above available to the Province on view-only access basis via secure web access. For clarity, any limitation on Province's inspection rights under this Section will not limit the Province's rights under any other provision of this Schedule to access or obtain copies of reports, records and other documentation.

19. STANDARD FOR SECURITY CONTROLS

(a) Except as this Agreement may specify otherwise, Service Provider must apply security controls to manage Confidential Information, Service Provider's Systems and Service Provider's Facilities, and the Services and related deliverables, that are compliant with all applicable Province Policies, including:

(i) the Province's "Information Security Policy" as may be accessed from the website of the Office of the Chief Information Officer (which, as of the Effective Date, is located at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/information-security-policy-and-guidelines); and

(ii) the Province's "IM/IT Standards" as may be accessed from the website of the Office of the Chief Information Officer (which, as of the Effective Date, is located at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/im-it-standards).

(b) Security policies, standards and procedures of the Province are subject to change in the Province's discretion and without notice. However, no additional requirement (including a higher standard) will form part of the Province Policies unless added in accordance with the applicable change process, if any, in this Agreement. For clarity, the Province may grant an exception to compliance with an additional requirement that forms part of the Province Policies.

(c) If an additional requirement of the Province Policies is added in accordance with the applicable change process, if any, in this Agreement, the Province agrees to pay any costs of Service Provider to implement changes to comply with an additional requirement to the Province Policies provided that Service Provider must not charge the Province an amount more than:

(i) once, to implement the same change to comply with the same additional requirement under different agreements between the parties, despite any provision in any agreement to the contrary; and

(ii) Province pre-approved, material, incremental costs actually incurred, including out of pocket costs and reasonable time charges based on Good Industry Practice.

20. OPEN SOURCE SOFTWARE

Unless the Province gives its prior written consent in or under this Agreement after being advised of the applicable license and affected work product or code, Service Provider must not:

(a) provide any work product (including Province Works) that derives from, consists of, embeds or incorporates any free or open source software (including freeware, but excluding public domain software) or provide any Service that introduces free or open source software into any of the Province's Systems or computer code (whether or not owned by or licensed to the Province); or

(b) use any free or open source software to create, modify, assemble, compile, produce or otherwise develop any work product (including Province Works) if it would require the work product or any of the Province's Systems or computer code (whether owned by or licensed to the Province) to:

(i) be made accessible or distributed in source code form to others;

(ii) be licensed to others for the purpose of making derivative works;

(iii) be licensed to others under terms that permit reverse engineering, reverse assembly or disassembly or other study for any purpose; or

(iv) be redistributable to others at no charge.

Any use of open source software must comply with the Province's "Guidelines on the Use of Open Source Software" as may be accessed from the website of the Office of the Chief Information Officer (which, as of the Effective Date, is located at https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/im-it-standards).

21. PRIVACY AND SECURITY CONTACT

Service Provider (but not a Subcontractor, Supplier or Managed Supplier) must provide in writing to the Province contact information for a Services Worker who will coordinate Service Provider's and

Subcontractors, Suppliers and Managed Suppliers' compliance and act as a direct contact for the Province on matters related to this Schedule and the Privacy Protection Schedule.

22. TERMINATION OF AGREEMENT

In addition to any other rights of termination the Province may have under this Agreement or at law, the Province may, subject to any applicable provision in this Agreement setting a mandatory cure period for default, terminate this Agreement on written notice to Service Provider if Service Provider fails to comply with this Schedule in a material respect.

23. APPROVED DISCLOSURE, ACCESS AND STORAGE OF SENSITIVE INFORMATION OUTSIDE CANADA

Service Provider will be permitted to disclose, access and store in the United States the Sensitive Information processed by the SP IMS applications identified as having processing and storage facilities in the United States in Appendix 3 (Systems Comprising SP IMS) of Schedule M (Service Provider IMS), which for clarity will not include any Personal Information, but only to the extent disclosure, access and storage is required by Service Provider to provide those applications and the Services in accordance with this Agreement.

24. USER IDENTIFICATION, AUTHENTICATION AND ACCESS MANAGEMENT

Service Provider must:

(a) comply with the Province's OCIO Identity Management and Security Standards (as may change from time to time, subject to Section 19(b)), which, as of the Effective date, is available at:

https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/im-it-standards

(b) ensure its systems used to provide the Services (including the SP IMS) utilize the Province's Enterprise Security Gateway services and technology for user identity, authentication, common logon, and user management support (or any successor services and technology for user identity, authentication, common logon, and user management support implemented by the Province) and integrates with such services and technology in a manner Approved by the Province;

(c) not use lightweight directory access protocol (LDAP) integration with identity directories, the collecting of username and password within any Province systems (including the Province IMS) or the use of solution specific user accounts;

(d) ensure its systems used to provide the Services (including the SP IMS) have the ability to identify a user using a unique identifier provided by the service and technology described in Section 24(b), which must have no visible identification qualities and must not be displayed to the user;

(e) ensure that all system-to-system communications require strong mutual authentication between the communicating systems (e.g. certificate based), including the existing direct system-to-system integrations, and the future use of enterprise integration platform (EIP);

(f) ensure that system-to-system communication attempts are restricted to authorized systems through the use of firewall rules;

(g) with respect to user authentication, Service Provider will use:

(i) brokered federation with the Province with use of an encrypted SAML token for personnel authentication that includes information similar to information included in a business card and must be sent via encrypted channels; or

(ii) if a PIA or STRA determines such solution is not viable, another authentication solution Approved by the Province.

25. NO STANDING ACCESS - REQUEST BASED ACCESS TO CUSTOMER DATA

Service Provider must ensure that:

(a) it implements software technologies and/or processes that restrict administrative access to data, systems and services with an ability to require Province approval before Service Provider can access the Province's data to perform support, maintenance or operational activities on any environment, system or service;

(b) any request by Service Provider personnel to access the Province environment (for support, maintenance, or operational purposes) goes through an approval workflow that requires approval from the Province; and

(c) Service Provider Personnel do not have Standing Access rights to Province data (i.e. data that is Province Information), and access to provide technical or customer support is only done with Approval from the Province.

26. ACCESS TO SECURITY REPORTS

Upon the Province's request, Service Provider must provide the Province with access to, and copies of, security reports for Service Provider systems processing or otherwise Handling data that is Province Information (including the Service Provider IMS); provided, however, that Service Provider will be entitled to redact or exclude from such reports any information which if disclosed to the Province would result in a breach of Service Provider's legal obligations (including confidentiality obligations) to any third party other than a Supplier, Managed Supplier or Subcontractor.

27. REMEDIATION OF DEFICIENCIES

If a security scan or report identifies any material vulnerabilities or other deficiencies in Service Provider systems processing or otherwise Handling data that is Province Information (including the Service Provider IMS), Service Provider will correct or sufficiently mitigate the deficiencies within the following applicable period based on the severity level of the deficiency:

(a) for a critical deficiency, within 72 hours of Service Provider learning of the deficiency;

(b) for a high deficiency, within 14 days of Service Provider learning of the deficiency; and

(c) for a medium or low deficiency, within 30 days of Service Provider learning of the deficiency.

For greater certainty, the foregoing would not apply to a PaaS or IaaS subcontractor to the extent that the vulnerability or deficiency is not in respect of or related to the Handling of Province Information (i.e. it would not apply to the subcontractor merely resolving service incidents generally relating to systems processing).

28. ATTESTATION OF COMPLIANCE

Upon request by the Province but no more than once per year, a senior officer of Service Provider will provide a written certificate to the Province attesting to Service Provider's compliance with Article 4.7 of the main body of this Agreement and this Schedule. For greater certainty, the Province does not require attestations from Service Provider subcontractors under this Section 28, just from Service Provider in respect of Service Provider and its subcontractors' compliance (where applicable) with Article 4.7 of the main body of this Agreement and this Schedule.

29. CONTINUOUS ACCESS OF PROVINCE TO PROVINCE DATA

At all times during the Term, the Province will have the ability to access and extract all or any portion of the data that is Province Information hosted or stored, directly or indirectly, by Service Provider as part of the Services in a manner agreed by the Parties. Service Provider will assist the Province in accessing data that is Province Information (including for purposes of extraction and deletion) in the event that any such data is not accessible to the Province through its use of the Services or the Service Provider IMS in accordance with this Agreement.

30. RESTRICTED ACCESS OF HOSTING PROVIDERS TO PROVINCE DATA

Service Provider represents and warrants to the Province that, to its best of knowledge, Service Provider's suppliers and subcontractors hosting data that is Province Information will not be able to access such data in unencrypted form without Service Provider's assistance. Service Provider must only provide access to such data to such suppliers and subcontractors, and more specifically only to their personnel that require access to such data and only at the time required, only as strictly required to provide the Services in accordance with this Agreement. Service Provider must not provide or authorize any such required access of any such supplier or subcontractor, or assist any such supplier or subcontractor in any way to access, any data that is Province Information without providing reasonable advance notice to the Province.

31. BACKUPS AND RESTORES

Service Provider must ensure that:

(a) Service Provider has a backup policy that is documented, followed, reviewed, updated, and tested at least annually;

(b) backups are taken and tested in accordance with Service Provider's backup policy, but in any event at least annually; and

(c) frequency of data backups is no less frequent than every 24 hours unless Approved and backups are completed in accordance with reasonable industry practice.

32. DELETION OF PROVINCE DATA

(a) The Parties agree that the applicable Articles of the main body of this Agreement, will apply to all data that is Province Information, whether or not it is Province Confidential Information. Upon termination or expiry of any Subcontract or Supplier Contract, Service Provider must ensure that the Subcontractor or Supplier, as applicable, returns and deletes all data that is Province Information in its direct or indirect possession in accordance with such Articles.

(b) Service Provider must ensure that any data that is Province Information is deleted from the enterprise integration platform (EIP) when no longer required to support reliable message command and communications.

33. SURVEILLANCE AND PHYSICAL SECURITY DATA

(a) With respect to Province Properties, the Province will retain responsibility for: (i) surveillance with respect to physical security and physical security data; and (ii) the provisioning and de-provisioning of building access cards and parking permits.

(b) With respect to physical security systems for Province Properties, Service Provider will only be responsible (as part of the Services) for the maintenance and updates of the security system hardware.

(c) Service Provider will not have authorization to change any of the existing security systems currently in place across the Province Properties.

(d) Service Provider will not have access to the security data stored by any security system for Province Properties

(e) Any change to Service Provider's responsibilities related to surveillance with respect to physical security and physical security data will be addressed through the Contract Change Process and undergo a privacy and security review at that time.

34. INTERPRETATION

(a) In this Schedule, unless otherwise specified, references to Sections are to Sections of this Schedule.

(b) Unless otherwise specified, any reference to the "Service Provider" in this Schedule includes any subcontractors or agents, whether directly or indirectly retained by Service Provider, involved in providing the Services, including all Subcontractors, Suppliers and Managed Suppliers, and Service Provider must ensure that any such subcontractors or agents comply with this Schedule to the extent that it applies to Services they are providing (including in all cases where any such subcontractor or agent will or could handle Province Confidential Information).

(c) If there is a conflict between a provision in an Appendix to this Schedule and the main body of this Schedule, the provision in the main body of this Schedule is inoperative to the extent of the conflict unless the provision in the main body of this Appendix states that it operates despite a conflicting provision in an Appendix to his Schedule.

(d) Sections 14 to 18, Section 32 and any other obligations of Service Provider in this Schedule (including any Appendix) which, by their terms or nature, are intended to survive the completion of the Services or termination of this Agreement, will continue in force indefinitely even after this Agreement ends.

II. Service Provider Personnel Security Screening - *applicable to Service Provider Personnel on site at a Client Facility*

For purposes herein, the following terms shall have the following meaning: "Service Worker" shall mean "Service Provider Personnel"; and "Province" shall mean "Client" or "CBRE".

1.0 VERIFICATION OF NAME, DATE OF BIRTH AND ADDRESS

Service Provider must verify the name, date of birth and current address of a Services Worker by viewing at least one piece of "primary identification" of the Services Worker and at least one piece of "secondary identification" of the Services Worker* that has not expired, as described in the table below. Subject to applicable laws, Service Provider must keep records of those verifications. For a Services

Worker from another province or jurisdiction, reasonably equivalent identification documents are acceptable.

Primary Identification	Secondary Identification
Issued by ICBC: • BC Services Card (photo) • Combination driver's licence and BC Services Card (photo) • B.C. driver's licence or learner's licence (photo) • B.C. Identification (BCID) card (not without expiry date) **Issued by provincial or territorial government:** • Canadian birth certificate **Issued by Government of Canada:** • Canadian Citizenship Card • Canadian Record of Landing/Canadian Immigration Identification Record • Passport • Permanent Resident Card • Secure Certificate of Indian Status (must have holographic design)	• Bank card (only if holder's name is imprinted and signed on card) • BC Services Card (non-photo) • B.C. CareCard or other health card issued by province or territory • Canadian or U.S. driver's licence • Canadian Forces ID • Correctional Service Conditional Release Card • Credit card (only if holder's name is imprinted on card) • Department of National Defense 404 driver's license (name, signature and photo) • Employee ID with photo • Firearms Acquisition Certificate • Foreign Affairs Canada or consular identification • Foreign birth certificate (a baptismal certificate is not acceptable) • Native Status card • Naturalization certificate • NEXUS card (name and photo) • Parole Certificate ID • Passport (Canada or foreign, including U.S. passport card) • Police identification • Student card (School ID) • Social Insurance Card (must have signature strip) • Vehicle registration (only if signed)

* It is not necessary that each piece of identification viewed by Service Provider contains the name, date of birth and current address of the Services Worker. It is sufficient that, in combination, the identification viewed contains that information.

2.0 VERIFICATION OF EDUCATION AND PROFESSIONAL QUALIFICATIONS

Service Provider must verify, by reasonable means, any relevant education and professional qualifications of a Services Worker, and keep records of those verifications.

3.0 VERIFICATION OF EMPLOYMENT HISTORY AND REFERENCE CHECKS

Service Provider must verify, by reasonable means, any relevant employment history of a Services Worker, which will generally consist of Service Provider requesting that a Services Worker provide employment references and Service Provider contacting those references. If a Services Worker has no relevant employment history, Service Provider must seek to verify the character or other relevant personal characteristics of the Services Worker by requesting the Services Worker to provide one or more personal references and contacting those references. Service Provider must keep records of those verifications.

4.0 SECURITY INTERVIEW

Service Provider must allow the Province to conduct a security-focused interview with a Services Worker if the Province identifies a reasonable security concern and notifies Service Provider it wishes to do so.

5.0 CRIMINAL HISTORY CHECK

Service Provider must arrange for and retain documented results of a criminal history check on a Services Worker obtained through the Services Worker's local policing agency. Criminal history checks must be repeated as necessary to ensure that at all times the most recent criminal history check on a Services Worker was completed within the previous five years.

If the results of the criminal history check on a Services Worker is not a clean record, Service Provider must:

(a) Even if Service Provider deems that the Service Worker does not constitute an unreasonable security risk, Service Provider must provide the criminal history check record of such Service Worker to the Province for evaluation to assist the Province in determining if it considers such Service Worker an unreasonable security risk;

(b) The Province reserves the right to refuse the use of such Service Worker in being involved in the provision of the Services or in accessing Confidential Information; and

(c) Service Provider must receive approval in writing from the Province that such Service Worker may be involved in the provision of the Services or in accessing Confidential Information.

APPENDIX 1

Intentionally Deleted.

APPENDIX 2

ADDITIONAL TERMS AND CONDITIONS

1.0 FIREWALL (STATEFUL INSPECTION FIREWALL)

Service Provider will ensure that stateful packet inspection firewalls will be implemented to control traffic flow to and from Service Provider's Systems, Facilities and Systems, at all times, and will be configured using industry best practices, and following the principles of least privilege.

2.0 IPS (INTRUSION PREVENTION SYSTEM)

Service Provider will ensure that IPS will be implemented to control and filter traffic flow leaving and entering Service Provider's Systems, Facilities and Systems, at all times, and will be configured using industry best practices.

3.0 APPLICATION FIREWALL - APPLICATION LAYER (LAYER 7) FILTERING

Service Provider will ensure that Application firewall - application layer (Layer 7) filtering will be implemented to protect applications that require such protection, as determined through the Security Threat and Risk Assessment conducted for the specific application and commensurate to the level of risk, as well as the security classification of the data being stored in the application or system. The application firewall is required to detect and mitigate application attacks such as, without limitation, brute force, OWASP Top 10, SQL injection, cross site scripting.

4.0 LOGGING OF SECURITY EVENTS

Service Provider will ensure that logging of Security Event Logs is enabled on all relevant infrastructure elements (such as, but not limited to firewall, IPS, L7 Application Firewall, Routers, Switches, Servers (OS, Security, IIS), Database, Web Servers, Application etc.).

During the Transition In Period, the Parties will agree on the Security Event Logs that will configured and enabled in Service Provider's devices, Systems and software that will be used to provide the Services as of the Service Commencement Date, provided, however, that the configured and enabled Security Event Logs will be consistent with Good Industry Practice. Following the Service Commencement Date, Service Provider must provide notice to the Province prior to making any changes to the configured and enabled Security Event Logs. If the Province determines, acting reasonably, that any such change would adversely impact the Province or the Services and notifies Service Provider of that determination, Service Provider will promptly meet with the Province to discuss whether the Services can be exempted from the change. If Service Provider does not grant to the Province an exemption from the change, Service Provider will be required to request the implementation of the change as it applies to the Services as a Change in accordance with the Contract Change Process. Notwithstanding the foregoing, Service Provider must always maintain sufficient Security Event Logs to comply with its obligations under this Schedule and Service Provider is not entitled to make any change to Security Event Logs that conflicts with its obligations under this Schedule.

5.0 SECURITY EVENT LOG RETENTION

Service Provider will ensure that the Security Event Logs are retained for a minimum period of 2 years.

6.0 MONITORING

Service Provider will ensure that automated tools will be implemented for the monitoring, review, correlating and alerting of Security Event Logs.

7.0 SECURITY INVESTIGATIONS SUPPORT

Service Provider will provide adequate support to the Province in conducting its own investigations into Information Incidents. This support will include, but not limited to, access to Security Event Logs for the Province security investigators and auditors in case of security investigations and audits. Access to such logs will be provided via an on-line, real-time GUI (Graphical User Interface) facility to permit timely access to logs. If such on-line access to logs is not possible due to technical limitations, Service Provider will provide access to logs via other methods, such as, but not limited to on-site visits to enable direct access to logs, log file requests, etc.

8.0 DOCUMENTATION OF PROCESSES AND PROCEDURES

Service Provider will ensure that all its security processes and procedures are documented adequately.

9.0 LOGICAL ISOLATION OF DATA

Without limiting any other obligations of Service Provider under this Agreement with respect to segregation or isolation of data (including hard copy Province Information), Service Provider will ensure that logical isolation of Province's data, including Sensitive Information, will be in place and configured at all times, and the logical isolation will remain in effect even in the case of equipment/technology failure.

10.0 ACCESS CONTROLS

Without limiting Service Provider's obligations under Section 6 of the main body of this Schedule, Service Provider will ensure that adequate access controls (i.e. Passwords, etc.) are in place and active at all times.

11.0 SERVER HARDENING

Service Provider will ensure that all operating systems on servers must be hardened against attack and misuse, using appropriate industry standard or best practice guidance for the hardening of the specific deployed platform, prior to being placed into production. On all server platforms, Service Provider will ensure all unsecured, unneeded and un-necessary ports, services and network communicating applications are un-installed or disabled. Using the principle of least privilege only ports, services and applications based on the functional requirements and required for the specific server will be configured and made operational.

12.0 ANTI-VIRUS AND ANTI-MALWARE

Service Provider will ensure that all servers will have antivirus/malware protection configured, active and enabled at all times. At a minimum, antivirus/malware definitions must be updated daily. At a minimum, servers must be configured to undergo a full anti-virus scan for latent infections (i.e. not previously detected by the real-time agent) on at least a weekly basis.

13.0 VULNERABILITY SCANNING

Service Provider will ensure that all servers will undergo a vulnerability scan before being placed into production after being built. Any vulnerability identified by such a scan will be remedied before the servers are placed into production. Service Provider will scan all Systems and Facilities providing the Services to which this schedule applies (such as, but not limited to, servers, databases, applications, routers, firewalls, IPS and switches, and all associated infrastructure used to manage and monitor the Services) for vulnerabilities on a regular basis, with a scanning schedule set at a minimum of one scan per quarter, unless otherwise Approved by the Province.

14.0 WEB APPLICATION VULNERABILITY SCANNING

Service Provider will ensure that all web applications are subjected to application vulnerability scanning before being placed into production, and any vulnerabilities or deficiencies identified are remedied before placing into production. Web application vulnerability scanning will be completed before any major changes to the application are implemented to ensure no vulnerabilities are introduced and any vulnerabilities and deficiencies identified are remedied before placing into production.

Web application will be scanned on a regular schedule thereafter, at a minimum of one scan per year, unless otherwise Approved by the Province.

15.0 PATCHING

Service Provider will ensure that devices, Systems or Facilities that provide the Services have all patches installed on a regular schedule, within the time frame recommended by the vendor, or as defined as a service level agreement in the contract. Service Provider will ensure that vulnerabilities are remedied and patches installed on an accelerated/emergency basis for zero-day, critical and high vulnerabilities. For zero-day vulnerabilities Service Provider will implement appropriate mitigation measures promptly on notification of the zero-day vulnerability. Service Provider will obtain information in a timely basis about technical vulnerabilities related to all information systems comprising the Systems, Facilities, infrastructure and the management network. Service Provider will implement processes to stay current with security threats identified in the industry.

16.0 WORKSTATION SECURITY

Service Provider will ensure that the workstations and other end-user devices that are used in the management, administration or access of the devices, Systems or Facilities that provide the Services, are protected adequately.

Such workstations will have appropriate antivirus protection active at all times, and antivirus scans are configured for a scan to be undertaken weekly at a minimum. All such workstations will have all patches and appropriate security updates completed regularly on the operating system and all software installed on the workstations at a minimum monthly.

17.0 PHYSICAL SECURITY

Service Provider will ensure that adequate physical controls and processes are implemented to ensure that only authorized personnel have physical access to Service Provider's infrastructure, Systems, management network, and its physical management ports.

18.0 CHANGE CONTROL

Service Provider will ensure that change control processes are implemented and maintained in line with applicable industry best practices and standards to reduce security-related risks with respect to implemented significant changes. Service Provider will ensure that adequate testing of any change is completed either before or during the implementation of such change but before being put into production.

19.0 ASSET DISPOSAL

Service Provider will ensure that all assets disposal related to the Services will be done in a secure manner.

APPENDIX 3

ADDITIONAL TERMS AND CONDITIONS FOR SYSTEMS UTILIZNG CLOUD SERVICES

1. DEFINITIONS

In this Appendix,

(a) "**Audit Record**" means audit records and Security Event Logs such as events, notifications or alerts that a device, system or software is technically capable of producing in relation to its status, functions and activities. Audit Records are not limited to security devices, but are applicable to all devices, systems and software that are technically capable of producing audit or event logs that can be used in security investigations, security incidents, auditing and monitoring. Examples of systems that can produce security audit records or event logs are, but are not limited to: firewalls, intrusion prevention systems, routers, switches, content filtering, network traffic flow logs, networks, authentication services, directory services, DHCP, DNS, hardware platforms, virtualization platforms, servers, operating systems, web servers, databases, applications, application/layer 7 firewalls;

(b) "**FIPS**" is an acronym for a Federal Information Processing Standard issued by NIST;

(c) "**IaaS Infrastructure**" means the infrastructure for IaaS that is managed by Service Provider (as referenced in Table 1) and that is used to provide the IaaS Tenancy including the systems, networks, hardware and software that are used by Service Provider to manage, operate and provide the IaaS;

(d) "**IaaS Tenancy**" means the IaaS service components and infrastructure (as referenced in Table 1, below) that are customer facing and that are managed by the customer in its use of IaaS, or are related to customer data or customer tenancy activities;

(e) "**Infrastructure as a Service**" or "**IaaS**" means a type of cloud service model having IT operations as the primary consumer and the following attributes, as published and more particularly described in the NIST CC Definition:

> The capability provided to the customer is to provision processing, storage, networks, and other fundamental computing resources, where the customer is able to deploy and run arbitrary software which can include operating systems and applications. In IaaS, the customer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g. host firewalls).

(f) "**must**" or "**required**" means, without limitation to other language of obligation, that the requirement is mandatory;

(g) "**NIST**" is an acronym for the National Institute of Standards and Technology, an agency of the U.S. Department of Commerce;

(h) "**NIST CC Definition**" means the NIST definition of cloud computing given in: National Institute of Standards and Technology, The NIST Definition of Cloud Computing (NIST Special Publication 800-145) (Gaithersburg, MD: National Institute of Standards and Technology, an agency of the U.S. Department of Commerce, 2011) (by Peter Mell and Timothy Grance), located, as of the Effective Date, online at http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf;

(i) "**NIST SP**" means NIST Special Publication and, unless the context otherwise provides, refers to the most current, non-draft, release of the specified Special Publication (located, as of the Effective Date, online at http://csrc.nist.gov/publications/PubsSPs.html or http://csrc.nist.gov);

(j) "**Platform as a Service**" or "**PaaS**" means a type of cloud service model having a developer/deployer as the primary consumer and the following attributes, as published and more particularly described in the NIST CC Definition:

> The capability provided to the customer is to deploy onto the cloud infrastructure customer-created or acquired applications created using programming languages, libraries, services, and tools supported by Service Provider. The customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment. [footnote omitted]

(k) "**PaaS Infrastructure**" means the infrastructure for PaaS that is managed by Service Provider including the systems, infrastructure, hardware and software that are used to manage, operate and provide the PaaS Infrastructure;

(l) "**PaaS Tenancy**" means the PaaS service components and infrastructure (as referenced in Table 1 of this Appendix) that are customer facing and that are managed by the customer in its use of PaaS, or are related to customer data or customer tenancy activities;

(m) "**PI Information**" means any Personal Information, and any cloud service derived data that could potentially identify a specific individual but that is not Personal Information that is subject to the *Freedom of Information and Protection of Privacy Act*, British Columbia;

(n) "**SaaS Infrastructure**" means the infrastructure for SaaS that is managed by Service Provider (as referenced in Table 1 of this Appendix) and that is used to provide the SaaS Tenancy, including the systems, infrastructure, hardware and software that are used to manage, operate and provide the SaaS Infrastructure;

(o) "**SaaS/PaaS/IaaS Infrastructure**" means collectively the SaaS Infrastructure, the PaaS Infrastructure and the IaaS Infrastructure;

(p) "**SaaS/PaaS/IaaS Tenancy**" means collectively the SaaS Tenancy, the PaaS Tenancy and the IaaS Tenancy;

(q) "**SaaS Tenancy**" means the SaaS service components and infrastructure (as referenced in Table 1 of this Appendix) that are customer facing and that are managed by the customer in its use of SaaS or are related to customer data or customer tenancy activities;

(r) "**should**" or "**recommended**" means that a stated security requirement is recognized by the Province as a good industry practice; and

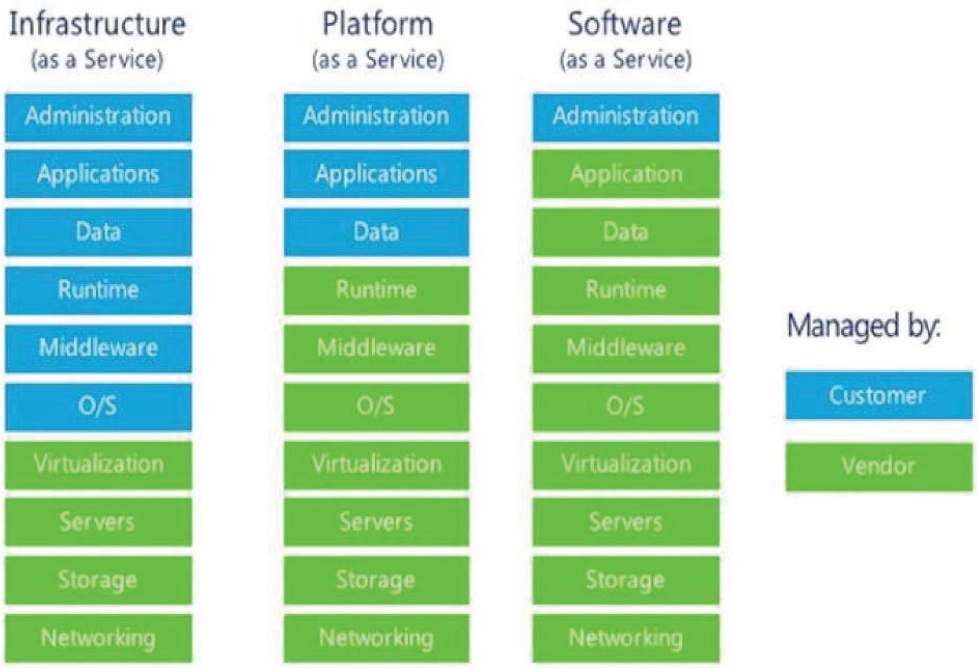
(s) "**Software as a Service**" or "**SaaS**" means a type of cloud service model having an end user as the primary consumer and the following attributes, as published and more particularly described in the NIST CC Definition 2011):

> The capability provided to the customer is to use the Service Provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based

email), or a program interface. The customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user specific application configuration settings. [footnote omitted]

Unless otherwise specified, all references to "sections" or "sub-sections" in this Appendix will refer to a section or sub-section of this Appendix.

Table 1 – Service management responsibility breakdown for the three types of services: IaaS, PaaS and SaaS.



2. PROVINCE APPROVAL REQUIRED TO UTILIZE CLOUD SERVICES

Service Provider must obtain approval in writing from the Province to utilize cloud services in the provision of Services.

3. COMPLIANCE AND CERTIFICATIONS

Service Provider must ensure that:

(a) the cloud services, the infrastructure providing the services, the management infrastructure used to manage the cloud services and all data centres used in providing the cloud services (including for management, back-up or disaster-recovery purposes) are compliant with one or more of the following established security standards, to the then current version:

(i) ISO/IEC 27017, demonstrated via certification with accreditation; OR

(ii) NIST SP 800-53, demonstrated via certification with accreditation; OR

(iii) Level 2 of Cloud Security Alliance (CSA) Security Trust and Assurance Registry (STAR) Certification as evidenced by a CSA audit report or letter from a CSA auditor, as may be defined on the CSA's website, which, as of the Effective Date, can be accessed at https://cloudsecurityalliance.org.

(b) Despite section 3(a), Service Provider may from the Effective Date until the earlier of the date that is six months after the Service Commencement Date, or such time as Service Provider complies with section 3(a), instead comply with all of the following:

(i) ISO/IEC 27001 demonstrated via certification with accreditation; AND

(ii) Level 1 (Self-Assessment) of the CSA STAR Program as described on the CSA's website at https://cloudsecurityalliance.org, with the information in the registry being current (submitted or modified within the past 18 months);

AND

(iii) Service Provider must provide evidence of additional certifications, if undertaken by Service Provider.

Service Provider must provide the Province with a status report regarding its progress towards complying with section 3(a) of this Security Schedule every six months from the Effective Date and until the earlier of its date of compliance and the date that is six months after the Service Commencement Date.

4. COMPLIANCE VERIFICATION AND ATTESTATION

Service Provider acknowledges and agrees that that the certification with accreditation to the standards in section 3(a) of this Appendix is the preferred method by the Province for Service Provider demonstrating its compliance with the Province's security requirements. In addition:

Service Provider must ensure that:

(a) it maintains at all times current certification with accreditation for the compliance with the standards listed in section 3(a);

(b) at the request of the Province or at a minimum annually, it provides the Province with evidence satisfactory to the Province that Service Provider is maintaining current certification with attestation for the compliance with the standards listed in section 3(a); and

(c) if certification with accreditation is not yet implemented by the CSP to demonstrate compliance with section 3, then the following alternate verification and attestation of compliance may be used:

(i) an annual SOC 2 Type II audit, conducted by an independent, accredited or otherwise reputable third-party auditor;

(A) the SOC 2 Type II audit must be appropriately scoped and conducted against the relevant principles and requirements, while choosing an appropriate framework for assessing the CSP's internal controls;

(B) the preferred control frameworks to be used when performing the SOC2 Type II audit are NIST SP 800-53, ISO/IEC 27017, CSA CCM;

OR

(ii) an annual Level 2 of CSA STAR Attestation as evidenced by a CSA audit report or letter from a CSA auditor, as may be defined on the CSA's website, which, as of the Effective Date, may be accessed at https://cloudsecurityalliance.org (or more particularly, at https://cloudsecurityalliance.org/star/#_overview).

Service Provider acknowledges and agrees that:

(d) audits that are not focused on evaluating an organization's information systems relevant to security, availability, integrity, confidentiality or privacy, are not considered sufficient or satisfactory by the Province as those audits may not adequately validate the security controls and security practices of an organization. For example, audits focused on an organization's internal controls that affect the organization's financial reporting (e.g. SAS70, SSAE16 SOC 1, etc.) are not considered sufficient by the Province; and

(e) audits that do not include the details of the controls implemented (e.g. SOC 3 audits/reports) to meet the necessary security requirement and as such do not allow the Province to assess the suitability of the cloud services, are not considered sufficient by the Province.

5. PRIVACY RELATED COMPLIANCE AND CERTIFICATIONS

Service Provider must ensure that in the case of systems handling or storing PI Information, Service Provider implements security standards related to PI Information handling, such as ISO/IEC 27018.

6. AUDIT RIGHTS RELATED TO SECURITY REQUIREMENTS

The compliance standards referenced in section 3(a), which require Service Provider to have accredited certification or appropriate audits, focus on framework control level only. In many certification standards, the details of the actual implementation of a control statement are purposely left undefined with the expectation and requirement that the data owner provide such details (as, for example, with requirements that are captured in international standards with terms such as "Organization Defined" [NIST SP 800-53] or "Cloud Service Customer defined" [ISO/IEC 27017] or "An Organization should" [ISO/IEC 27002]).

Service Provider acknowledges and agrees that any certification and accreditation audit to the standards in section 3(a) will not necessarily validate the necessary implementation details or provide clarity as to whether Service Provider has implemented the cloud service security controls in a matter that mitigates risk at a level acceptable to the Province. For example, it is not sufficient that a third party certification audit validates that a control is implemented if the third party certification audit did not validate the frequency and other parameters that determine if the control is effective in mitigating risk:

> Example: "malware scans are undertaken regularly" versus "malware scans are undertaken regularly and at a minimum of once per week".

Consideration by the Province of the adequacy of the security parameters in Service Provider's services will therefore require that audits of third party certification or accreditation validate the Province's specific parameters: generic terms such as "regular", without customer specificity, will not be sufficient.

In addition to any other audit rights the Province may have, Service Provider must ensure that the Province is provided with a process that allows the Province to validate Service Provider's compliance

with Service Provider's security obligations under this Appendix, if such compliance is not otherwise evidenced by a certification audit. The following provisions will apply to any such process:

(a) the Province may initiate an audit of Service Provider's compliance with the security obligations under the Agreement and this Appendix up to once a year, through the use of its own independent, third party, industry recognized auditor;

(b) the Province will review audits undertaken by Service Provider to determine if individual controls are addressed in an existing audit report performed by a qualified third-party auditor within the prior twelve months, provided that Service Provider confirms that there are no known material changes in the controls audited. The Province agrees to accept those findings in lieu of requesting an audit of the controls, but only if the audit of the control is covered at the necessary level of detail to validate the compliance with the respective section in this Appendix or otherwise in this Agreement, if applicable. If at any time the Province determines, in its sole discretion, that compliance with any applicable security obligation set forth in this Appendix or otherwise in this Agreement cannot be validated through information provided to the Province in connection with an audit conducted by Service Provider, then the Province reserves the right to require validation of such obligation through a third party Province initiated audit;

(c) the Province will provide an audit plan to Service Provider at least two weeks in advance of the proposed audit date. The audit plan will describe the proposed scope, duration, and start date of the audit;

(d) the audit will be conducted during regular business hours at the applicable Service Provider facility, subject to all reasonable Service Provider policies regarding third party access to Service Provider buildings or facilities, and will not unreasonably interfere with Service Provider's business activities;

(e) upon request from Service Provider, the Province will provide Service Provider with any audit reports generated by a Province initiated audits, unless prohibited by law. The audit reports will, subject to the provisions of the *Freedom of Information and Protection of Privacy Ac*t (British Columbia), be treated by the Province as Service Provider's confidential information; and

(f) Province initiated audits will be at the Province's expense.

7. ACCESS CONTROL

Service Provider must:

(a) implement an access control policy and associated access control procedures that address, without limitation, onboarding, off-boarding, transition between roles, regular access reviews, limit and control use of administrator privileges and inactivity timeouts;

(b) document, follow, review, and update Service Provider's access control policies and procedures at least every three years;

(c) ensure that all access to information and system functions is based on principles of "least privilege" and "need to know", and that employees, contractors or vendors are provided only with the access they are authorized to have in accordance with such principles;

(d) identify and segregate conflicting duties and areas of responsibility to reduce incidents of fraud and other abuse (e.g. separation of duties);

(e) review and update the current access control policy at least every three years;

(f) review and update the current access control procedures at least annually;

(g) ensure that when assigning a unique identifier for users, Service Provider validates the proper identification of the individual to whom the identifier is being issued, before giving the user access to systems;

(h) implement a formal user registration process;

(i) ensure that the user registration process includes verification of access levels, maintenance of records of access privileges, audit processes, and actions to ensure access is not permitted until formal approval is granted;

(j) ensure that the access control policy clearly states the information access privileges for each defined role in the organization;

(k) maintain a current and accurate inventory of computer accounts and review the inventory on a regular basis to identify dormant, fictitious or unused accounts;

(l) implement a formal process to assign defined roles to users;

(m) implement a monitoring process to oversee, manage and review user access rights and roles at regular intervals;

(n) at least annually, conduct access reviews and reviews of accounts for compliance with account management requirements;

(o) ensure that information systems:

(i) enforce a limit of not more than three consecutive invalid logon attempts by a user during a fifteen-minute time period; and

(ii) automatically lock the account/node for thirty minutes after a third consecutive login failure;

(p) limit the number of concurrent sessions to three sessions for privileged access and two sessions for non-privileged access;

(q) prevent further access to information systems by initiating a session lock after 15 minutes of inactivity;

(r) provide the capability of allowing remote access to the information system to be disconnected or disabled within 15 minutes of inactivity; and

(s) ensure that the information system automatically disables inactive user accounts after 90 consecutive days of inactivity.

8. AUTHENTICATION AND MULTI-FACTOR AUTHENTICATION

Service Provider must:

(a) implement multi-factor authentication for all administrative and privileged account access;

(b) change authentication passwords every 180 days at a minimum;

(c) ensure that the information system, for password-based authentication:

(i) enforces minimum password complexity, including requiring passwords to be case sensitive, contain a minimum of eight characters and at least one each of upper-case letters, lower-case letters, numbers, and special characters;

(ii) enforces at least one changed character when new passwords are created;

(iii) stores and transmits only encrypted representations of passwords;

(iv) enforces password minimum and maximum lifetime restrictions of one day minimum and 180-day maximum; and

(v) prohibits password reuse for 24 generations;

(d) ensure that information system identifiers are managed by:

(i) preventing reuse of identifiers for at least two years; and

(ii) disabling the identifier after ninety days of inactivity;

(e) develop, document, and disseminate an identification and authentication policy and procedures;

(f) review and update the current identification and authentication policy at least once every three years; and

(g) review and update the current identification and authentication procedures at least once annually.

9. <u>ADDITIONAL REQUIREMENT FOR AUTHENTICATION:</u>

Service Provider must:

<u>Specific to IaaS</u>:

Ensure that the IaaS Tenancy offers the technical capability to support two-factor authentication in order to allow the Province to have the technical capability to configure two-factor authentication for the IaaS Tenancy.

<u>Specific to PaaS</u>:

Ensure that the PaaS Tenancy offers the technical capability to support two-factor authentication in order to allow the Province to have the technical capability to configure two-factor authentication for the PaaS Tenancy.

<u>Specific to SaaS</u>:

Ensure that the SaaS Tenancy offers the technical capability to support two-factor authentication in order to allow the Province to have the technical capability to configure two-factor authentication for the SaaS Tenancy.

10. ADDITIONAL REQUIREMENT FOR SINGLE SIGN-ON AUTHENTICATION:

Service Provider must support single sign-on technologies for authentication (e.g. SAML 2.0 or equivalent).

11. SECURITY AWARENESS

Service Provider must ensure that:

(a) it documents, follows, reviews, and updates its security awareness and training policy, procedures, programs and courses;

(b) it reviews and updates its security awareness and training policies at least every three years;

(c) it reviews and updates its security awareness and training procedures at least annually;

(d) all Service Provider Personnel providing cloud services under this Agreement undergo information security training at Service Provider's expense as part of their initiation prior to providing any services to the Province and prior to the commencement of a new role with a different security classification, and thereafter at least on an annual basis;

(e) information security training educates users on common threats and impacts to business such as not sharing credentials, not clicking on suspicious links and attachments, reporting security incidents, maintaining clean desk, locking inactive systems, concealing valuables;

(f) all initial and annual security awareness training of its personnel includes security best practices, threat recognition, compliance and policy requirements, and reporting obligations; and

(g) the information security training complies with Section 5 of the main body of this Schedule.

12. LOG GENERATION

Service Provider must:

(a) develop, document, and disseminate audit and accountability policies and procedures;

(b) review and update its audit and accountability policies at least once every three years;

(c) review and update its audit and accountability procedures at least once annually;

(d) in order to ensure that logs are not lost due to component or system failure, configure all systems producing Audit Records to transfer logs at least daily to a separate centralized logging system that is a physically different system or system component than the system producing the Audit Records;

(e) configure all the systems producing Audit Records in such a manner that no logs are overwritten prior to transfer or backup to the centralized logging system;

(f) configure the backup or forwarding of logs to the centralized logging system for real-time or near real-time log backup or forwarding for networked components/systems;

(g) configure a maximum delay of one week or less for log backup or transfer from standalone systems or components;

(h) configure privileged and administrative account activity logging;

(i) protect the logs and the centralized logging facilities from unauthorized access, modification, and deletion; and

(j) notify the Province in all cases where Service Provider has disabled, partially disabled or not configured the generation of Audit Records that the components, systems and software are technically capable of producing. The Province will assess such partial or lack of logging to determine if the risk introduced by such partial or lack of logging is acceptable to the Province;

(k) *Specific to IaaS*:

(i) configure and enable the Audit Records logging that the IaaS Infrastructure is technically capable of producing to assist in the identification of compromises, breaches and incidents, in order to support security monitoring activities and to enable security investigations; and

(ii) ensure that the IaaS Tenancy offers the technical capability of generating comprehensive Audit Records for all elements, systems and software components of the IaaS Tenancy to allow the Province to have the technical capability to configure the generation of Audit Records for the IaaS Tenancy components, in order to support security monitoring activities and to enable security investigations;

(l) *Specific to PaaS*:

(i) configure and enable the Audit Records logging that the PaaS Infrastructure is technically capable of producing to assist in the identification of compromises, breaches and incidents, in order to support security monitoring activities and to enable security investigations; and

(ii) ensure that the PaaS Tenancy offers the technical capability of generating comprehensive application/activity/tenancy Audit Records for all elements, systems and software components of the PaaS Tenancy to allow the Province to have the technical capability to configure the generation of Audit Records or the PaaS Tenancy components, in order to support security monitoring activities and to enable security investigations;

(m) *Specific to SaaS*:

(i) configure and enable the Audit Records logging that the SaaS Infrastructure is technically capable of producing to assist in the identification of compromises, breaches and incidents, in order to support security monitoring activities and to enable security investigations; and

(ii) ensure that the SaaS Tenancy generates comprehensive application/activity/tenancy Audit Records for all elements, systems and software components of the SaaS Tenancy in order for the Province to support security monitoring activities and to enable security investigations.

Additionally:

(n) Service Provider must protect the confidentiality and integrity of the centralized logs using encryption.

(o) As part of the infrastructure logs Service Provider must implement flow information logging (e.g. session bytes transferred information, NetFlow, network traffic telemetry) or equivalent, so that in the case of a security breach, the quantity of exfiltrated data can be easily and readily determined.

(p) *Specific to IaaS*:

Service Provider must ensure the IaaS Tenancy offers the technical capability of generating flow information logs (e.g. session bytes transferred information, NetFlow, network traffic telemetry) or equivalent, so that the Province can enable the logging of flow information within the IaaS Tenancy in order to easily and readily determine the quantity of exfiltrated data in the case of a security breach.

13. LOG RETENTION

Service Provider must:

(a) *Specific to IaaS:*

(i) retain the Audit Records that the IaaS Infrastructure is producing to enable Service Provider to conduct security monitoring and security investigations into incidents, breaches and compromises;

(ii) retain Audit Records for the IaaS Infrastructure for a minimum of 90 days on-line;

(iii) retain Audit Records for the IaaS Infrastructure on-line or off-line for an additional period of time that is adequate to enable Service Provider to conduct effective security investigations into incidents, breaches and compromises; and

(iv) ensure that:

(A) the IaaS Tenancy retains the Audit Records that the IaaS Tenancy is producing such as OS, middleware, runtime, data, application, activity, tenancy, administration logs related to the Province data and Province user activities; OR

(B) the IaaS Tenancy has the technical capabilities to enable the Province to retain Audit Records in accordance with the record maintenance requirements of this Agreement.

(b) *Specific to PaaS*:

(i) retain the Audit Records that the PaaS Infrastructure is producing to enable Service Provider to conduct security monitoring and security investigations into incidents, breaches and compromises;

(ii) retain Audit Records for the PaaS Infrastructure for a minimum of 90 days;

(iii) retain Audit Records for the PaaS Infrastructure online or off-line for an additional period of time that is adequate to enable Service Provider to conduct effective security investigations into incidents, breaches and compromises;

(iv) retain Audit Records for the PaaS Tenancy for a minimum of 90 days; and

(v) ensure that the PaaS Tenancy retains the Audit Records that the PaaS Tenancy is producing, such as data/application/activity/tenancy/administration logs related to the Province data and Province user activities, or has the technical capability to enable the Province to retain the Audit Records in accordance with the records maintenance requirements of this Agreement.

(c) *Specific to SaaS*:

(i) retain the Audit Records that the SaaS Infrastructure is producing to enable Service Provider to conduct security monitoring and security investigations into incidents, breaches and compromises;

(ii) retain Audit Records from the SaaS Infrastructure for a minimum of 90 days;

(iii) retain Audit Records for the SaaS Infrastructure online or off-line for an additional period of time that is adequate to enable Service Provider to conduct effective security investigations into incidents, breaches and compromises;

(iv) retain the Audit Records that the SaaS Tenancy is producing, such as application/activity/tenancy/administration logs related to the Province data and Province user activities;

(v) retain Audit Records from the SaaS Tenancy for a minimum of 90 days; and

(vi) ensure that the SaaS Tenancy has the technical capabilities to enable the Province to retain the Audit Records in accordance with records maintenance requirements of this Agreement.

(d) *For SaaS, PaaS and IaaS*:

(i) retain the investigation reports and Audit Records related to a security investigation pertaining to SaaS/PaaS/IaaS Infrastructure or SaaS/PaaS/IaaS Tenancy for a minimum period of two years after the investigation is completed; and

(ii) provide the Province, at the Province's written request, with copies of relevant Audit Records and investigation reports related to security investigations pertaining to the SaaS/PaaS/IaaS Tenancy so that the Province may retain such relevant Audit Records or investigation reports in accordance with the records maintenance requirements of this Agreement.

14. LINE/GRAPHICAL USER INTERFACE (GUI) ACCESS TO LOGS

Service Provider must, where possible:

(a) specific to IaaS, ensure that the IaaS Tenancy has the technical capability to allow the Province to configure online GUI access to the Audit Records that are generated for the IaaS Tenancy to enable the Province to conduct timely and effective security investigations by searching/reviewing such logs;

(b) specific to PaaS, configure and provide online GUI access to the Audit Records that are generated for the PaaS Tenancy and ensure that a minimum of 90 days' worth of the most current logs are accessible through the on-line GUI interface to enable the Province to conduct timely and effective security investigations by searching/reviewing such logs; and

(c) specific to SaaS, configure and provide online GUI access to the Audit Records that are generated for the SaaS Tenancy and ensure that a minimum of 90 days' worth of the most current logs are accessible through the on-line GUI interface to enable the Province to conduct timely and effective security investigations by searching/reviewing such logs.

15. FORWARDING OF LOGS AND EXTRACTION OF LOGS

Service Provider must ensure that the SaaS/PaaS/IaaS Tenancy offers the technical capability for the Province to enable or configure the forwarding/extraction/backup of Audit Records from the SaaS/PaaS/IaaS Tenancy for forwarding/extraction/backup, no less frequently than every 24 hours, to the Province security information and event management system (SIEM) or to an external log storage and retention system.

16. MONITORING, AUDITING AND CORRELATION OF LOGS

Service Provider must:

(a) implement continuous, real-time monitoring of Audit Records from the available sources using automated tools such as a SIEM or equivalent;

(b) implement automated tools for real-time correlation, review, monitoring and alerting of Audit Records from the infrastructure providing or managing the cloud services;

(c) configure continuous review of system logs, audit, access records and Audit Records using automated tools and appropriate processes;

(d) ensure that Service Provider's incident response teams, tools and processes monitor the real-time alerts from the monitoring systems; and

(e) ensure that it implements privileged and administrative account activity monitoring and review.

17. INVESTIGATIONS SUPPORT AND SECURITY INVESTIGATIONS

(a) In addition to Service Provider's obligations under Section 15 of the main body of this Schedule, Service Provider must, at no additional cost to the Province, upon the Province's request, provide the Province with sanitized Audit Records from the SaaS/PaaS/IaaS Infrastructure to assist the Province in conducting its own security investigations.

(b) Service Provider will be entitled to redact or exclude from logs and other materials provided to the Province under this Section 17 or under Section 15 of the main body of this Schedule, other than audit reports, any information which if disclosed to the Province would result in a breach of Service Provider's legal obligations (including confidentiality) to a third party, other than a Supplier, Managed Supplier or Subcontractor.

18. E-DISCOVERY AND LEGAL HOLDS

Service Provider must ensure the SaaS/PaaS/IaaS Tenancy provides e-discovery and legal hold features for the Audit Records generated for the infrastructure and the services to enable the Province to conduct timely and effective cloud security investigations and meet judicial requests for legal holds.

19. NETWORK TIME PROTOCOL

Service Provider must ensure that, unless otherwise agreed by the Parties:

(a) all service infrastructure, devices and systems which are involved in the Handling of Sensitive Information is synchronized with a master network time server, that in turn is synchronized to authoritative Stratum time servers; and

(b) time synchronization occurs at least daily.

20. PENETRATION TESTING

Service Provider must ensure that:

(a) it conducts penetration tests of the cloud infrastructure regularly in line with reasonable industry practices and guidance; and

(b) it conducts penetration testing at least annually.

21. SEPARATION OF PRODUCTION FROM TEST ENVIRONMENTS

Service Provider must ensure that:

(a) development, test and training environments use clean test data unless otherwise Approved. If production data is needed for these environments, the data must be obfuscated, such as by using data masking functionality;

(b) it has the ability to perform obfuscation on data held in non-production environments; and

(c) development, test and training environments are separated from production environments, and the separation is maintained at all times, even in the case of equipment or technology failure.

If the Province Approves use of any production data, including Sensitive Information, in non-production environment, the non-production environment must have production grade controls that comply with this Schedule.

22. CHANGE CONTROL AND MANAGEMENT

Service Provider must ensure that:

(a) change control processes are implemented and maintained in accordance with reasonable industry practices and standards to reduce security-related risks with respect to implemented significant changes;

(b) adequate testing of any change is completed either before or during the implementation of such change but before being put into production;

(c) change control policy is documented, followed, reviewed, updated, and tested at least annually;

(d) changes to production environments are reviewed and approved by the appropriate authority at Service Provider; and

(e) changes to the system/service (not including data changes through the service) go through the change management process, including notification, testing, acceptance and implementation.

23. SYSTEMS AND SERVER HARDENING

For systems and server hardening:

(a) Service Provider must ensure that, for SaaS/PaaS/IaaS Infrastructure, it hardens all systems and servers against attack and misuse, using appropriate industry standards or practice guidance for the hardening of the specific deployed platform, prior to being placed into production.

(b) Service Provider must ensure that it un-installs or disables all unsecured and unneeded ports, services, applications, protocols and network communicating applications on all systems and servers. Using the principle of least privilege, Service Provider must ensure it only configures and makes operational ports, services, applications, protocols and applications based on the functional requirements of the specific system or server. Default passwords and shared accounts must not be used.

(c) Service Provider must implement domain specific security practices and controls in addition to the general framework controls and practices listed in the relevant sections of the compliance standards detailed in section 3(a) of this Appendix, as may be required by the Province. Service Provider must implement system and server hardening practices and controls that conform or comply with reasonable industry practices and relevant domain specific standards such as NIST SP 800-123 (Guide to General Server Security), CIS Benchmarks or equivalent.

(d) *Specific to IaaS*:

Service Provider must implement server hardening using industry recognized configuration guidelines such as CIS Benchmarks or equivalent for server operating systems (such as Windows, Linux, Unix) and server virtualization.

(e) *Specific to PaaS*:

Service Provider must implement server hardening using industry recognized configuration guidelines such as CIS Benchmarks or equivalent, for server operating systems (such Windows, Linux and Unix), server virtualization and server middleware (such as web servers and database servers).

(f) *Specific to SaaS*:

Service Provider must implement server hardening using industry recognized configuration guidelines such as CIS Benchmarks or equivalent, for server operating systems (such as Windows, Linux, Unix), server virtualization, server middleware (such as web servers and database servers) and application servers.

24. DATABASE SECURITY

Service Provider must:

(a) ensure that database maintenance utilities that bypass controls are restricted and monitored;

(b) ensure that there is a formal approval process in place for handling requests for disclosure of database contents or for database access. This process should include steps to evaluate privacy impacts and security risks of such request; and

(c) implement methods to check and maintain the integrity of the data (such as consistency checks and checksums).

For database security, Service Provider must implement logical isolation and encryption of Province information.

25. WORKSTATION SECURITY

Service Provider must ensure that all workstations used in the management and provision of the cloud services, and all workstations that are used to access the relevant infrastructure, will have appropriate antivirus protection active at all times, and that, at a minimum, the antivirus protection will be configured to perform antivirus scans once per week. All such workstations will have all patches and appropriate security updates completed monthly for the operating system and all software installed on the workstation.

26. CHANGES TO HOSTING ENVIRONMENT

Service Provider must ensure that it performs security testing of all significant changes to the hosting environment (such as operating system, database and applications) as part of the change management process for the hosting environment.

27. BUSINESS CONTINUITY PLAN AND DISASTER RECOVERY PLAN

Service Provider must ensure that:

(a) it has a business continuity plan that is documented, followed, reviewed, updated, and tested at least annually;

(b) it has a disaster recovery plan that is documented, followed, reviewed, updated, and tested at least annually; and

(c) it reviews and updates its business continuity plan and disaster recovery plan at least annually.

28. INCIDENT RESPONSE AND MANAGEMENT

Service Provider must ensure that:

(a) Service Provider's incident management policy is documented, followed, reviewed, updated, and tested at least annually;

(b) Service Provider's security incident response plan is documented, followed, reviewed, updated, and tested at least annually;

(c) Service Provider reviews and updates its incident management policy at least once every three years; and

(d) Service Provider reviews and updates its security incident response plan at least annually.

Additionally, Service Provider must implement security incident management practices and controls that conform or comply with reasonable industry practices and relevant domain specific standards such as NIST SP 800-61, ISO/IEC 27035, ISO/IEC 18044 or equivalent.

29. ASSET MANAGEMENT AND DISPOSAL

Service Provider must ensure that:

(a) all asset disposals related to the services are done in a manner that ensures that information cannot be recovered;

(b) Service Provider's asset management and disposal policy is documented, followed, reviewed, and updated regularly in line with reasonable industry practices and guidance, and includes hardware, software and other critical business assets;

(c) inventory includes the name of system, location, purpose, owner, and criticality;

(d) assets are added to inventory on commission and removed on decommission; and

(e) disposal requirements are based on the sensitivity of the information.

30. INFORMATION DESTRUCTION AND DISPOSAL

Service Provider must ensure that:

(a) information on magnetic media is destroyed by overwriting, degaussing or using some other adequate method; and

(b) it uses best practice procedures and adequate media wiping solutions when disposing of media.

Additionally, Service Provider must implement media sanitization practices and controls that conform or comply with industry best practices and relevant domain specific standards such as NIST SP 800-88, ISO/IEC 27040:Annex A or equivalent.

31. PHYSICAL SECURITY

Service Provider must:

(a) develop, document, and disseminate a physical and environmental protection policy;

(b) review and update its current physical and environmental protection policy at least once every three years;

(c) review and update its current physical and environmental protection procedures at least once annually; and

(d) review physical access logs at least once monthly.

32. INFORMATION SECURITY POLICY

Service Provider must ensure that:

(a) its information security policy is documented, approved, followed, reviewed, and updated at least every three years;

(b) its information security policy is based on recognized industry standards;

(c) it reviews and updates its information security policy at least once annually; and

(d) it has documented and implemented an acceptable use policy.

33. RISK ASSESSMENTS AND SECURITY REVIEWS

Service Provider must ensure that:

(a) threat and risk assessments are undertaken for new systems, infrastructure or services;

(b) threat and risk assessments are undertaken for significant changes to systems, infrastructure or services;

(c) it conducts security assessments at least annually, against an established security standard;

(d) threat and risk assessments are scheduled annually for existing systems, infrastructure and services;

(e) it documents and follows its then-current risk assessment policy and reviews and updates such risk assessment policy at least once every three years; and

(f) it reviews and updates its risk assessment procedures at least once annually.

34. VULNERABILITY MANAGEMENT AND PATCHING

Service Provider must:

(a) ensure that the software, devices, systems, infrastructure or facilities that provide or manage the services have all patches installed on a regular schedule in accordance with Service Provider's patching policy (but in any event following reasonable industry practices);

(b) ensure that vulnerabilities are remedied and patches installed on an accelerated/emergency basis for zero-day, critical and high vulnerabilities;

(c) implement appropriate mitigation measures promptly on notification of the zero-day and critical vulnerabilities;

(d) mitigate zero-day and critical vulnerabilities immediately or as soon as possible;

(e) remediate zero-day, high and critical vulnerabilities through patching, decommission, or compensating controls;

(f) patch high vulnerabilities within 30 days or less of discovery;

(g) patch medium vulnerabilities within 90 days or less of discovery;

(h) obtain information in a timely basis about technical vulnerabilities related to the software, devices, systems, infrastructure or facilities providing or managing the cloud services;

(i) implement processes to stay current with security threats identified in the IT industry;

(j) conduct all reasonable due diligence by regularly checking appropriate expert websites and vendor software websites for alerts about new vulnerabilities and patches;

(k) document, follow, review, and update a vulnerability management and patching policy on an ongoing basis;

(l) review and update the current vulnerability management and patching policy at a minimum of every three years;

(m) review and update the current vulnerability management and patching procedures at a minimum annually;

(n) patch all systems and software regularly in line with reasonable industry practices and guidance and ensure that current software, operating system and application levels are maintained; and

(o) conduct vulnerability assessments as part of a program and rate vulnerabilities according to criticality on an ongoing basis.

35. VULNERABILITY SCANNING

For vulnerability scanning:

(a) *IaaS/PaaS/SaaS*:

(i) Service Provider must conduct vulnerability scans for all SaaS/PaaS/IaaS Infrastructure components before any such components are put into production and after any major changes. Service Provider must remedy any vulnerabilities identified by the scan before rolling into production the identified infrastructure components.

(ii) Service Provider must implement vulnerability scans for all SaaS/PaaS/IaaS Infrastructure components when new vulnerabilities potentially affecting the systems and applications are identified and reported and Service Provider must remedy any vulnerabilities identified by the scan as appropriate.

(iii) Service Provider must scan for vulnerabilities all the SaaS/PaaS/IaaS Infrastructure components providing the services (such as, but not limited to, servers, databases, applications, routers, firewalls, switches, and all associated infrastructure used to manage and monitor the services) on a regular basis and Service Provider must implement a scanning schedule of a minimum of one vulnerability scan per month.

(iv) Service Provider must allow the Province or an Approved qualified third party to perform, and support the Province or the third party, as the case may be, in performing vulnerability scans of IaaS/PaaS/SaaS Tenancy to validate the security posture of the services.

(b) *Specific to IaaS*:

(i) Service Provider must ensure that the IaaS Tenancy has the technical capability to allow the Province or an Approved qualified third party to perform, enable or configure vulnerability scanning within the IaaS Tenancy.

36. WEB APPLICATION VULNERABILITY SCANNING

For web application vulnerability scanning:

(a) *Specific to SaaS/PaaS*:

Service Provider must:

(i) implement application vulnerability scanning for all web applications or web interfaces before they are put into production, and remedy any vulnerabilities or deficiencies identified before they are put into production;

(ii) implement application vulnerability scanning for all web application or web interfaces after any major changes to the web application or the web interface to ensure no vulnerabilities are introduced and vulnerabilities or deficiencies identified are remedied before being put into production;

(iii) implement regular, scheduled, application vulnerability scanning for web applications and web interfaces; and

(iv) ensure that web applications and web interfaces are scanned for vulnerabilities at least once per month.

(b) *Specific to IaaS*:

(i) Service Provider must ensure that the IaaS Tenancy has the technical capability to allow the Province to enable and configure web application vulnerability scanning within the IaaS Tenancy.

(c) *SaaS/PaaS/IaaS*:

(i) Service Provider must allow the Province or an Approved qualified third party to perform, and support the Province or the third party, as the case may be, in performing web application vulnerability scans of SaaS/PaaS/IaaS Tenancy to validate the security posture of the services.

37. PROVINCE STRA SUPPORT

In addition to Service Provider's obligations under Section 8(b) of the main body of this Schedule, Service Provider must ensure that:

(a) it provides the necessary documentation, including architecture diagrams, service architecture, security controls architecture, technical information (that may be sanitized by Service Provider to remove any proprietary or customer specific personal information) and support to the Province to enable the Province to complete a STRA of the cloud service and assess the risk associated with the service provided by Service Provider; and

(b) it provides the Province with required information and support via technical and security resources that can provide security and technical information regarding Service Provider cloud infrastructure and services implementation to enable the Province to assess security risks.

38. PERSONNEL SECURITY AND SECURITY SCREENING

Service Provider must ensure that it screens individuals prior to authorizing access to information systems.

39. SECURITY SCREENING AND CRIMINAL RECORDS CHECK REQUIREMENTS

In addition to, and without limiting, any other personnel security checks that the Agreement may require (including under Section 4 of the main body of this Schedule and Appendix 1 of this Schedule), Service Provider must ensure that:

(a) its Services Workers, including personnel who have access to any systems transmitting or storing Province information, complete a satisfactory criminal record check in accordance with Appendix 1 of this Schedule, which is updated at least every five years; and

(b) its Services Workers are required to proactively disclose criminal offences to Service Provider, unless prohibited by law.

40. SUPPLIER, CONTRACTOR AND SUBCONTRACTOR SECURITY REQUIREMENTS

Without limiting Service Provider's obligations under Article 5 (Suppliers & Managed Suppliers) and 7.2 (Use of Subcontractors for Services) of the main body of this Agreement, Service Provider must ensure that:

(a) the security requirements of its suppliers, contractors and subcontractors, including the security requirements of any subcontractors it uses to provide cloud services to the Province, are documented, followed, reviewed, and updated on an ongoing basis;

(b) it requires its suppliers, contractors and subcontractors to meet or exceed Service Provider's own security policies and comply with all applicable security requirements set out in this Agreement;

(c) it requires its suppliers, contractors and subcontractors, including any subcontractors it uses to provide cloud services to the Province, to demonstrate evidence of compliance;

(d) all supply chain security risks are identified, mitigated, and reviewed on an ongoing basis; and

(e) suppliers, contractors and subcontractors, including any third party customer support providers, are required to enter into contracts with Service Provider including confidentiality provisions, background screening requirements, training and breach of policy and enforcement provisions that comply with this Agreement.

41. APPLICATION DEVELOPMENT

Service Provider must ensure that:

(a) applications and programming interfaces are developed according to industry standards; and

(b) it uses secure development practices for the development of the SaaS/PaaS software.

42. ENCRYPTION

(a) Service Provider must:

(i) implement encryption of data at rest for the Province's information;

(ii) ensure that encryption of data at rest remains in effect, uninterrupted, and active at all times, even in the case of equipment or technology failure;

(iii) implement encryption for the transmission of data;

(iv) implement encryption for data in transit for all transmissions of Province information;

(v) ensure that the encryption for the transmission of data is end-to-end and the payload containing the Province information is not read or accessed anywhere on the transmission path via decrypting and parsing the payload containing the Province information;

(vi) implement encryption for all access and connectivity to the services;

(vii) implement encryption for all access and connectivity to the infrastructure;

(viii) notify the Province if encryption is not implemented or is less than the requirements in this section;

(ix) ensure that backup data that requires encryption is encrypted with AES with a minimum key length of 256 bits;

(x) ensure that it will not place any Province information on portable media for transport outside Service Provider data centre;

(xi) ensure that, if the Province agrees in writing to have its information transported via portable media outside Service Provider data centre, then all portable media must be encrypted as follows:

(A) the portable media must be certified by NIST to FIPS 140-2 Level 2 or above;

(B) all user writeable partitions on the drive must be fully encrypted;

(C) the encryption algorithm must be AES as per the NIST - FIPS 197 Advanced Encryption Standard;

(D) the AES encryption key must be a minimum of 256 bits long;

(E) the device must lockdown after consecutive failed login attempts;

(F) the number of failed login attempts must not exceed 12;

(G) the USB flash drive must enforce the use of a complex password; and

(H) for information with a security classification of high, the portable media must be certified by NIST to FIPS 140-2 Level 3.

(b) When configuring encryption, Service Provider must ensure that it follows the Province's Cryptographic Standards for Information Protection, which, as of the Effective Date, are available at:

https://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/im-it-standards

Additionally for encryption, Service Provider must:

(c) *Specific to IaaS*:

(i) ensure that the IaaS Tenancy offers the technical capability of cryptographic key management to allow the Province to have the technical capability to manage encryption keys for the IaaS Tenancy; and

(ii) not hold or have access to the encryption keys if they are managed by the Province and used to encrypt the Province's information.

(d) *Specific to PaaS*:

(i) ensure that the PaaS Tenancy offers the technical capability of cryptographic key management to allow the Province to have the technical capability to manage encryption keys for the PaaS Tenancy; and

(ii) not hold or have access to the encryption keys if they are managed by the Province and used to encrypt the Province's information.

(e) *Specific to SaaS*:

(i) ensure that the SaaS Tenancy offers the technical capability of cryptographic key management to allow the Province to have the technical capability to manage encryption keys for the SaaS Tenancy; and

(ii) not hold or have access to the encryption keys if they are managed by the Province and used to encrypt the Province's information.

43. ISOLATION CONTROLS AND LOGICAL ISOLATION OF DATA

Service Provider must:

(a) implement and maintain the logical isolation of the Province's information;

(b) ensure that logical isolation remains in effect, uninterrupted, and active at all times, even in the case of equipment or technology failure;

(c) implement, where supported by available technology, the logical isolation of Audit Records related to Province information and activities;

(d) ensure that logical isolation of Audit Records remains in effect at all times, even in the case of equipment or technology failure;

(e) segregate all tenancy traffic from management network traffic at all times;

(f) segregate traffic of different tenants from each other using logical isolation technologies like firewalls, VLANs, MPLS or equivalent; and

(g) ensure that tenancy isolation is maintained at all times, even in the case of equipment or technology failure.

44. PERIMETER CONTROLS (FIREWALL + INTRUSION PREVENTION SYSTEM) AND NETWORK SECURITY

Service Provider must:

(a) implement stateful packet inspection firewalls to control traffic flow to and from Service Provider's systems, infrastructure, data centre, SaaS/PaaS/IaaS Infrastructure and SaaS/PaaS/IaaS Tenancy at all times, and configure the stateful packet inspection firewalls using industry best practices, and following the principles of least privilege;

(b) implement an intrusion prevention system to control and filter traffic flow leaving and entering Service Provider's systems, infrastructure, data centre, SaaS/PaaS/IaaS Infrastructure and SaaS/PaaS/IaaS Tenancy at all times, and configure the intrusion prevention system using industry best practices; and

(c) implement a secure network perimeter and network segmentation, with ingress/egress points that are known and controlled.

45. APPLICATION (LAYER 7) FIREWALL

Service Provider must ensure that a web application firewall - application layer (Layer 7) filtering will be implemented to protect web applications. The web application firewall must detect and mitigate application attacks such as, without limitation, brute force, OWASP Top 10, OWASP Core rule set 3.0/2.2.9, SQL injection, cross site scripting.

46. AVAILABILITY OF SECURITY CONTROLS

Service Provider must have a security architecture for cloud services that, at minimum, provides the capability to enable/configure the applicable controls listed below and, based on architecture diagrams, the security architecture is Approved by the Province.

(a) *Specific to IaaS*:

(i) the service offers the capability to enable/configure security controls within the IaaS Tenancy such as:

(A) network firewalls;

(B) intrusion prevention systems;

(C) host based firewalls;

(D) antivirus;

(E) application (Layer 7) firewalls;

(F) encryption and key management;

(G) SIEM;

(H) vulnerability scanning; and

(I) log retention facilities;

(ii) the service offers the capability to enable/configure logging and retention of Audit Records from such security controls;

(b) *Specific to PaaS*:

(i) the service offers the capability to enable/configure security controls within the PaaS Tenancy such as:

(A) application (Layer 7) firewalls;

(B) Encryption and key management; and

(C) Log retention facilities;

(c) *Specific to SaaS*:

(i) the service offers the capability to enable/configure security controls within the SaaS Tenancy such as:

(A) encryption and key management; and

(B) log retention facilities.

47. MANAGEMENT NETWORK AND INFRASTRUCTURE

Service Provider must ensure that:

(a) the management network remains logically separated from any other zone and is not directly accessible from the Internet;

(b) the management network is internally segmented, with each server's dedicated network interface on its own segmented network and that interfaces on the management network do not have visibility to each other; and

(c) all access to the management network is strictly controlled and exclusively enforced though the use of a secure access gateway or bastion host.

48. SECURITY ZONES

Service Provider must ensure that the service infrastructure has policy enforcement points (firewalls) controlling access between zones.

49. REMOTE MANAGEMENT AND SECURE ACCESS GATEWAY

Service Provider must ensure that:

(a) all management access uses a two-factor authentication;

(b) all administrative access to any of the services and their respective applications is routed through a secure access gateway that restricts the flow of information from the management zone;

(c) there is no direct connectivity into the server zones for management activities or for direct file transfer from workstations;

(d) it logs and monitors all administrative access to all applications and supporting systems;

(e) it implements a two-factor authentication for the secure access gateway; and

(f) it reviews the secure access gateway logs at a minimum on a monthly basis for evidence of misuse or abuse of privileges.

50. DISTRIBUTED AND DENIAL OF SERVICE ATTACK PROTECTION

Service Provider must ensure that it implements and maintains distributed denial of service attack protection of the SaaS/PaaS/IaaS Infrastructure and SaaS/PaaS/IaaS Tenancy as follows:

(a) Network Layer - Layer 3 DDOS protection; and

(b) Application Level – Layer 7 DDOS protection if applicable.

51. ANTIVIRUS AND MALWARE

Service Provider must ensure that:

(a) *Specific to IaaS*:

(i) the IaaS Tenancy has the technical capability to allow the Province to enable and configure antivirus and malware protection within the IaaS Tenancy;

(b) *Specific to PaaS*:

(i) the PaaS Tenancy has the technical capability to allow the Province to enable and configure antivirus and malware protection within the PaaS Tenancy;

(c) *Specific to SaaS*:

(i) the SaaS Tenancy has antivirus and malware protection configured and active within the SaaS Tenancy at all times;

(d) *SaaS/PaaS/IaaS*:

for the SaaS/PaaS/IaaS Infrastructure:

(i) all relevant servers have antivirus and anti-malware protection installed, configured, active and enabled at all times;

(ii) antivirus and anti-malware definitions are updated daily;

(iii) all relevant servers are configured to undergo a full anti-virus and anti-malware scan for infections on at least a weekly basis; and

(iv) anti-virus and anti-malware protection are implemented on all relevant Windows operating system servers.

(e) *SaaS/PaaS/IaaS*:

Service Provider must ensure that it implements antivirus and anti-malware protection on all relevant Linux and Unix operating system servers.

52. NOTIFICATIONS OF BREACHES

Service Provider must notify the Province immediately of Service Provider's identification of a potential or actual breach or incident that may affect the Province's information, tenancy or SaaS/PaaS/IaaS Tenancy, including any Information Incident.

53. NOTIFICATIONS OF CHANGES TO POLICIES, AGREEMENTS, INFRASTRUCTURE, SECURITY CONTROLS, SECURITY PROFILE

Service Provider must notify the Province of any changes to its security policies, procedures or agreements referenced in this Appendix or otherwise in this Agreement and will provide such notice in accordance with Section 2.4 of Schedule M where such Section is applicable.

The Province reserves the right to determine, at its sole discretion, if changes by Service Provider to its security policies, procedures or agreements have introduced unacceptable security risk for the Province or have decreased the Province's required security for SaaS/PaaS/IaaS Tenancy; and Service Provider acknowledges and agrees that the Province may avail itself of any termination rights in this Agreement on a non-fault or for cause basis in the event that the Province deems any such changes by Service Provider to have introduced an unacceptable security risk or to have decreased the Province's required security for the services.

54. SECURITY ANALYTICS

Service Provider must ensure that it implements security analytics solutions as part of its monitoring activities to increase the security of the cloud infrastructure and services.

55. ENHANCED LOGGING TECHNOLOGIES

Service Provider must ensure that the service implements or supports enhanced logging and logs all access to Personal Information and sensitive data.

56. DIGITAL RIGHTS MANAGEMENT

Service Provider must ensure that the service implements or supports digital rights management or rights management service technologies.

57. DATA LOSS PREVENTION

Service Provider must ensure that the service implements or supports data loss prevention technologies.

58. SECURITY ENHANCING PRACTICES

Service Provider must ensure that it undertakes additional activities to test and enhance the security of the infrastructure and services, such as security simulations, war game simulations, red team/blue team testing and disaster recovery simulations.

59. DATA STORAGE AND DATA ACCESS RESIDENCY REQUIREMENTS:

Service Provider must ensure that:

(a) all Province information and data, and logs related to Province information and data, are stored at data centres located in Canada except as otherwise permitted under Section 23 of the main body of this Schedule;

(b) no access to Personal Information is from outside of Canada, and no disclosure of Personal Information is made outside of Canada;

(c) unless otherwise agreed by the Province within the Privacy Protection Schedule, maintenance activities that may access Personal Information are performed from within Canada; and

(d) it configures data storage, including log files, to remain in one region and that its system does not replicate/failover outside of that region.

60. REPORTS

Service Provider must ensure that:

(a) at no additional cost and at the request of the Province, Service Provider will generate the following security reports every six months and provide such reports to the Province:

(i) vulnerability scan reports of the infrastructure providing the cloud services, including all network equipment providing the cloud services; and

(ii) patch status reports for the infrastructure providing the cloud services.

61. RESTRICTED ACCESS OF HOSTING PROVIDERS TO PROVINCE DATA

Service Provider represents and warrants to the Province that, to its best of knowledge, Service Provider's suppliers and subcontractors hosting data that is Province Information in a cloud services environment will not be able to access, or will have difficulty isolating and accessing, such data in unencrypted form without Service Provider's assistance. Service Provider must only provide access to such data to such suppliers and subcontractors, and more specifically only to their respective personnel that require access to such data and only at the time required, only as strictly required to provide the Services in accordance with this Agreement. Service Provider must not provide or authorize any such required access of any such supplier or subcontractor, or assist any such supplier or subcontractor in any way to access, any data that is Province Information without providing reasonable advance notice to the Province.

62. INSPECTION

With respect to cloud services, notwithstanding Section 18 of the main body of this Schedule X, the Province will not be entitled under that Section to enter on the premises of any cloud services provider to inspect any documentation or records without the agreement of the cloud services provider, but the Province will remain entitled to inspect all of the documentation and records described in that Section by obtaining copies, to the extent permitted under that Section, or through remote access in accordance with that Section.

APPENDIX 4

AUDITS AND INSPECTIONS OF SUPPLIERS

1. Significant Supplier Contracts

Significant supplier contracts are an agreement (e.g. purchase orders, agreements or other forms), entered into or to be entered into that satisfies one or more of the following criteria ("**Significant Supplier Contracts**"):

- For cleaning or housekeeping, if the total contract value exceeds $250,000 (exclusive of Taxes);
- If the contract value exceeds $1 million per year (exclusive of Taxes);
- All Services procured for Critical Environments;
- For all Agreements, where the Service to be provided to the Province Properties is greater than $50,000 (exclusive of Taxes);
- In the case of a commitment which relates to the provision of utilities to a Province Property by an entity that is not a governmental or other similar public authority (such utility supply contracts requiring the Province's approval are being referred herein as "**Utility Contracts**"); and
- Any other commitment that the Province has identified.

The Province will have the right to review Significant Supplier Contracts prior to the commitments being entered into by Service Provider.

The Province will have the right to review the proposed termination of Significant Supplier Contracts, and, prior to a new or renewed a Significant Supplier Contract being entered into by Service Provider, will have the right to review any such new or renewed Significant Supplier Contract.

In connection with seeking Province's review for any Significant Supplier Contract, Service Provider will provide all documentation that is necessary to satisfy the Province, including any direct or indirect costs that are to be assumed by the Province, Suppliers or Managed Supplier. Service Provider and the Province will establish the process to be used for the review of identified Significant Supplier Contracts. By reviewing any such agreement, the Province accepts no liability for such agreement.

2. Audits and Inspections of Suppliers

1. All Significant Supplier Contracts will include provisions giving the Province, its internal and external auditors and its professional advisors a right to perform audits and inspections with respect to those specific aspects of the Significant Supplier's operations that pertain to the Services, to the extent permitted by, and in accordance with, the provisions contained herein. In addition, all Significant Supplier Contracts will contain provisions naming the Province as an intended beneficiary of such audit rights. Service Provider agrees that:

    a. in the case of Significant Supplier Contracts that are entered into after the Effective Date, Service Provider will include provisions in such Significant Supplier Contracts that comply with this Article; and

    b. in the case of Significant Supplier Contracts which were entered into before the Effective Date and do not include provisions complying with this Article, Service Provider will negotiate amendments to such Significant Supplier Contracts to insert such provisions into the Significant Supplier Contracts within six (6) months of the Effective Date.

2. For Supplier Contracts which are not Significant Supplier Contracts, Service Provider will include in such Supplier Contracts, where practicable, provisions giving the Province, its internal and external auditors and its professional advisors a right to perform audits and inspections with respect to those specific aspects of the Supplier's operations that pertain to the Services. In addition, where practicable, such contracts will contain provisions naming the Province as intended beneficiary of such audit rights.

3. In the event that it is not practicable to include the provisions contemplated by Article in a Supplier Contract, Service Provider will provide such assistance (including the exercise by Service Provider of its audit rights under such Supplier Contract) to the Province, its internal and external auditors and its professional advisors as may be required to perform such audits and inspections, as necessary, with respect to those specific aspects of the Supplier's operations that pertain to the Services.

4. In addition to the other rights set out above in this Article, Service Provider agrees that the Province will have a right, from time to time, to conduct an investigation of a Supplier, including reviewing the Supplier's practices, interviewing the Supplier's personnel, inspecting the Supplier's premises and obtaining information and documents from the Supplier, to confirm that the Supplier is following the requirements of this Agreement relating to Security Clearance Check or the security, confidentiality or treatment of Province Confidential Information. Service Provider will assist the Province and ensure that the Supplier cooperates in such an investigation.

PRIVACY PROTECTION SCHEDULE

1. DEFINITIONS

Capitalized terms used and not otherwise defined in this Schedule will have the meaning set out it the Agreement. For purposes of this Schedule, the following words and terms will have the following meanings:

(a) "**access**" means disclosure by the provision of access;

(b) "**Act**" means the *Freedom of Information and Protection of Privacy Act*;

(c) "**Anonymization**" means a de-identification process that removes or transforms all direct and indirect identifiers in a record for which there is a reasonable or realistic possibility that the identifiers could be used, either alone or with other information, to identify an individual, and "**Anonymize**" and "**Anonymized**" will have a correlative meanings. For clarity, for a record to be Anonymized, it must no longer contain any personal information.

(d) "**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;

(e) "**personal information**" means recorded information about an identifiable individual, other than contact information, collected or created by, or on behalf of, Service Provider as a result of this Agreement or any previous agreement between the Province and Service Provider dealing with the same subject matter as this 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; and

(f) "**privacy course**" means:

(i) the Province's online privacy and information sharing training course, as may be updated and replaced from time to time; or

(ii) another Approved equivalent privacy and information sharing training course, that addresses, at a minimum:

(A) definition of personal information/personally identifiable information;

(B) breach/incident identification and reporting;

(C) appropriate access/use/handling of personal information/personally identifiable information;

(D) principles of need-to-know and least-privilege; and

(E) reasonable security measures/arrangements.

For clarity, any such equivalent privacy and information sharing training course could be delivered by Service Provider provided that it is Approved by the Province.

2. PURPOSE

The purpose of this Schedule is to:

(a) enable the Province to comply with the Province's statutory obligations under the Act with respect to personal information; and

(a) ensure that, as a service provider, Service Provider is aware of and complies with Service Provider's statutory obligations under the Act with respect to personal information.

3. ACKNOWLEDGEMENTS

Service Provider acknowledges and agrees that:

(b) all personal information is Province Information and, therefore, all provisions of this Agreement applicable to Province Information apply to personal information (except where there is a conflict between this Schedule and the obligations applicable to the Province Information, in which case this Schedule will govern);

(c) the Act applies to the operation of the SP IMS and all other Services provided under this Agreement;

(d) it is a "service provider" (as that term is defined in the Act); and

(e) it is responsible for the actions and omissions of Service Provider Resources and for their compliance with the Privacy Obligations and Service Provider will ensure each subcontractor (including Suppliers and Subcontractors) or agent of Service Provider who may access personal information will comply with the Act and acknowledge it is a "service provider" (as that term is defined in the Act).

4. COLLECTION OF PERSONAL INFORMATION

Unless this Agreement otherwise specifies or the Province otherwise directs in writing, Service Provider may only access, collect or create personal information that is necessary for the performance of Service Provider's obligations, or the exercise of Service Provider's rights, under this Agreement.

Unless this Agreement otherwise specifies or the Province otherwise directs in writing, Service Provider must collect personal information directly from the individual the information is about.

Unless this Agreement otherwise specifies or the Province otherwise directs in writing, Service Provider must tell an individual from whom Service Provider collects personal information, in a form Approved by the Province:

(f) the purpose for collecting it;

(a) the legal authority for collecting it;

(b) the title, business address and business telephone number of the person designated by the Province to answer questions about Service Provider's collection of personal information; and

(a) any other information required by the Province from time to time.

5. PRIVACY TRAINING

(a) Service Provider must ensure that each person (including Service Provider Personnel) who will provide services under this Agreement that involve the collection, creation or other Handling of personal information will complete, at Service Provider's expense, a privacy course prior to that person providing those services.

(b) The requirement in section 5(a) will only apply to persons who have not previously completed the privacy course.

6. ACCURACY OF PERSONAL INFORMATION

Service Provider must make every reasonable effort to ensure the accuracy and completeness of any personal information to be used by Service Provider or the Province to make a decision that directly affects the individual the information is about.

7. REQUESTS FOR ACCESS TO PERSONAL INFORMATION

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

8. CORRECTION OF PERSONAL INFORMATION

(a) Within five (5) Business Days of receiving a written direction from the Province to correct or annotate any personal information, Service Provider must annotate or correct the information in accordance with the direction.

(b) When issuing a written direction under section 8(a), the Province must advise Service Provider of the date on which the correction request to which the direction relates was received by the Province in order that Service Provider may comply with section 8(c).

(c) Within five (5) Business Days of correcting or annotating any personal information under Section 8(a), Service Provider must provide the corrected or annotated information to any party to whom, within one year prior to the date on which the correction request was made to the Province, Service Provider disclosed the information being corrected or annotated.

(d) If Service Provider receives a request for correction of personal information from a person other than the Province, Service Provider must promptly advise the person to make the request to the Province and, if the Province has advised Service Provider of the name or title and contact information of an official of the Province to whom such requests are to be made, Service Provider must also promptly provide that official's name or title and contact information to the person making the request.

9. PROTECTION OF PERSONAL INFORMATION

Without limiting Service Provider's obligations under Article 4.7 of the main body of this Agreement and Schedule X (Security), Service Provider 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 this Agreement.

10. STORAGE AND ACCESS TO PERSONAL INFORMATION

Unless the Province otherwise directs in writing, Service Provider must not store personal information outside Canada or permit access to personal information from outside Canada.

11. RETENTION OF PERSONAL INFORMATION

Unless this Agreement otherwise specifies, Service Provider must retain personal information until directed by the Province in writing to dispose of it or deliver it as specified in the direction.

12. USE OF PERSONAL INFORMATION

(a) Unless the Province otherwise directs in writing, Service Provider may only use personal information if that use is for the performance of Service Provider's obligations, or the exercise of Service Provider's rights, under this Agreement. Notwithstanding the foregoing, if Service Provider becomes aware that it has received or collected any personal information in the Service Provider IMS, Service Provider must not use that Personal Information and, in accordance with the Information Incident process under Schedule X (Security), must permanently delete that personal information in accordance with the data deletion requirements of this Agreement.

(b) For clarity, "use of personal information" includes Anonymizing, aggregating or otherwise Handling personal information for the purpose of generating non-personal information and analyzing personal information (including by manual and automated means), including for the purpose of developing insights, conclusions and other information from personal information, and such use of personal information is prohibited under this Agreement, except as expressly permitted under Section 21 of this Schedule or Article 11.8 of the main body of this Agreement. All Anonymization permitted under this Agreement must be performed on the Province IMS unless otherwise Approved. Further, Service Provider will not Handle any personal information for any of the following purposes, any or all of which are not required for the performance of Service Provider's obligations, or the exercise of Service Provider's rights, under this Agreement: (i) advertising, marketing or other commercial purpose for any Person other than the Province; or (ii) augmenting or enhancing Service Provider's or any subcontractor's customer profiles of End Users other than as required to perform the Services.

13. DISCLOSURE OF PERSONAL INFORMATION

(a) Unless the Province otherwise directs in writing, Service Provider may only disclose personal information inside Canada to any person other than the Province if the disclosure is for the performance of Service Provider's obligations, or the exercise of Service Provider's rights, under this Agreement.

(b) Unless this Agreement otherwise specifies or the Province otherwise directs in writing, Service Provider must not disclose personal information outside Canada.

14. NOTICE OF FOREIGN DEMANDS FOR DISCLOSURE

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

(g) receives a foreign demand for disclosure;

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

(b) has reason to suspect that an unauthorized disclosure of personal information has occurred in response to a foreign demand for disclosure.

Service Provider must immediately notify the Province 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.

15. NOTICE OF UNAUTHORIZED DISCLOSURE

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

16. INSPECTION OF PERSONAL INFORMATION

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

17. COMPLIANCE WITH THE ACT AND DIRECTIONS

(a) Service Provider must in relation to personal information comply with: (i) the requirements of the Act applicable to Service Provider as a service provider, including any applicable order of the commissioner under the Act; and (ii) any direction given by the Province under this Schedule provided that Service Provider's compliance with such direction is technically feasible (cost implications excluded). To the extent that compliance with any such direction imposes costs upon Service Provider, the Province agrees to pay the costs of Service Provider to comply with such direction, provided that Service Provider must not charge the Province an amount more than Province pre-approved, material, incremental costs actually incurred, including for out of pocket costs and reasonable time charges based on Good Industry Practice.

(b) Service Provider acknowledges that it is familiar with the requirements of the Act governing personal information that are applicable to it as a service provider.

(c) Service Provider will provide the Province with such information as may be reasonably requested by the Province from time to time to assist the Province in confirming that the SP IMS and the Services comply with the Act and the Province's security policies.

18. NOTICE OF NON-COMPLIANCE

If for any reason Service Provider does not comply, or anticipates that it will be unable to comply, with a provision in this Schedule in any respect, Service Provider must promptly notify the Province 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.

19. TERMINATION OF AGREEMENT

In addition to any other rights of termination which the Province may have under this Agreement or otherwise at law, the Province may, subject to any provisions in this Agreement establishing mandatory cure periods for defaults by Service Provider, terminate this Agreement by giving written

notice of such termination to Service Provider, upon any failure of Service Provider to comply with this Schedule in a material respect.

20. ATTESTATION OF COMPLIANCE

Upon request by the Province but no more than once per year, a senior officer of Service Provider will provide a written certificate to the Province attesting to Service Provider's compliance with this Schedule.

21. SERVICE SPECIFIC PRIVACY RISK MITIGATIONS

Service Provider represents, warrants and covenants to the Province that, as of the Effective Date and throughout the Term, the Service Provider IMS (including all applications comprising the Service Provider IMS) is not intended to collect, store or access any personal information and Service Provider will not intentionally use the Service Provider IMS to collect, store or access any personal information.

22. INTERPRETATION

(a) In this Schedule, references to sections by number are to sections of this Schedule unless otherwise specified in this Schedule.

(b) Any reference to the "Service Provider" in this Schedule includes any subcontractors or agents, including Subcontractors, Suppliers, Managed Suppliers, retained by Service Provider to perform obligations under this Agreement (whether directly or indirectly) that involve any possible or actual Handling of personal information and Service Provider must ensure that any such subcontractors and agents comply with this Schedule.

(c) The obligations of Service Provider in this Schedule will survive the termination of this Agreement.

(d) If a provision of this Agreement (including any direction given by the Province under this Schedule) conflicts with a requirement of the Act or an applicable order of the commissioner under the Act, the conflicting provision of this Agreement (or direction) will be inoperative to the extent of the conflict.

(e) Service Provider must comply with the provisions of this Schedule despite any conflicting provision of this Agreement or, subject to section 22(f), the law of any jurisdiction outside Canada.

(f) Nothing in this Schedule requires Service Provider to contravene the law of any jurisdiction outside Canada unless such contravention is required to comply with the Act.

SUPPLEMENTARY CONDITIONS
TO CCDC-2 (2008)

CONTRACT BETWEEN CBRE LIMITED, AS OWNER
AND TBA. Zoom invitation to follow **, AS CONTRACTOR**

DATED: _____

GENERAL REFERENCE

The following Supplementary Conditions shall be read in conjunction with the Standard Construction Document, CCDC-2 (2008).

The form of Agreement between CBRE Limited as (the "Owner") and Contractor to be signed is the pre-printed Standard Construction Document, CCDC-2 (2008), Stipulated Price Contract.

Section and paragraph references below are to the corresponding sections and paragraphs of the Agreement between CBRE Limited as (the "Owner") and Contractor, Definitions and General Conditions of the Standard Construction Document, CCDC-2 (2008), Stipulated Price Contract.

FOR CLARITY, ALL REFERENCES IN THE CCDC-2 (2008) TO "OWNER" SHALL MEAN AND REFER TO CBRE LIMITED. REFERENCES TO CLIENT SHALL MEAN OWNER'S CLIENT. UNLESS OTHERWISE PROVIDED IN THE CONTRACT DOCUMENTS, TO THE EXTENT THE OWNER HAS A CONTRACTUAL OBLIGATION WITH A CLIENT WHERE THE CONTRACT DOCUMENTS ARE FOR THE BENEFIT OF THE CLIENT, ALL RIGHTS, TITLE AND INTEREST IN THE CONTRACT, INCLUDING THE WORK AND PRODUCTS SHALL INURE TO THE BENEFIT OF SUCH CLIENT.

AGREEMENT BETWEEN OWNER AND CONTRACTOR

Article A-2 AGREEMENT AND AMENDMENTS

2.3 Add a new paragraph 2.3 as follows:

Contractor agrees to be bound by and to assume for the benefit of the *Owner* all of the obligations and responsibilities that the *Owner* assumes for the benefit of the *Owner* and its client with respect to the Project as set forth in this Agreement. All Work shall be subject to the *Owner's client* Required Contract Flow-Down Provisions as set forth in Exhibit 1.

Article A-4 CONTRACT PRICE

4.3 Delete 4.3 and replace with:

The total amount payable by the *Owner* to *Contractor* for the construction of the Work is guaranteed by the *Contractor* not to exceed $ _____ ."

Article A-5 PAYMENT

5.4 Add a new paragraph 5.4 as follows:

"Notwithstanding anything to the contrary contained in this Agreement or the Contract Documents, *Owner* shall make payment of all undisputed amounts within forty five (45) days (or such time period as may be required by Applicable Law) after receipt of proper invoice containing all required information and documentation as required by *Owner* in its sole discretion provided however, that notwithstanding the foregoing, or any language to the contrary contained in this Agreement, to the extent permitted by Applicable Law, *Owner* shall have no obligation for the payment of any portion of the *Contract Price*, including, but not limited to, progress payments, for *Products* and *Services* provided and the *Work* performed and satisfactorily completed by the *Contractor* until the *Owner* has received payment from the *Owner's* client for such portions of the *Contract Price* due to *Contractor*.

DEFINITIONS
Amend Definition 1 "Change Directive", by adding the following language to the end of the definition:

"The *Consultant's* standard form document shall be used."

Amend Definition 4, "Consultant", by adding the following language to the end of the definition:

"For purposes of the Contract, the terms "*Consultant*", "Architect", and "Engineer" shall be considered synonymous."

Add a new definition 27 "OHSA", as follows:

"27. **OHSA**
'OHSA' means the Occupational Health and Safety Act (based on the respective provincial legislation or authority having jurisdiction where the *Work* is being conducted)."
Add the following definitions:

"28. **Confidential Information**

Confidential Information means any information of the Disclosing Party that is not generally known to the public and at the time of disclosure is identified, or would reasonably be understood by the Receiving Party, to be proprietary or confidential, whether disclosed in oral, written, visual, electronic or other form, and which the Receiving Party (or in the case of Contractor its subcontractors or agents) observes or learns in connection with this Agreement. Confidential Information includes, but is not limited to: (a) business plans, strategies, forecasts, projects and analyses; (b) financial information and fee structures; (c) business processes, methods and models; (d) customer, tenant, employee and supplier information; (e) materials, product and service specifications; (f) manufacturing, purchasing, logistics, sales and marketing information; and (g) the terms and conditions of this Agreement. Confidential Information also includes Personal Information and Client Data.

29. **Disclosing Party**

Disclosing Party means the Party or Client providing Confidential Information to the Receiving Party.

30. **Receiving Party**

Receiving Party means the Party receiving Confidential Information from the Disclosing Party."

THE GENERAL CONDITIONS OF THE STIPULATED PRICE CONTRACT

GC 1.1 CONTRACT DOCUMENTS

1.1.8 Delete paragraph 1.1.8 in its entirety and substitute new paragraph 1.1.8:

"1.1.8 The *Owner* shall provide the *Contractor*, without charge, one copy of the *Contract Documents*.

All *Drawings* and *Specifications* are to be returned to the *Owner* at the end of the *Project*, including contract sets, issued for construction sets and progress drawings issued by the *Consultant*. In the event such materials are not returned to the *Owner* at the time of *Project* close out, a deduction will be made from funds owing to the *Contractor*. The cost of returning such materials to the *Owner* is an expense of the *Contractor*. Upon notice in writing to the *Owner*, the *Contractor* may retain some or all of such materials to support its warranty obligations under the *Contract* and shall deliver such retained materials to the *Owner* upon completion of its warranty obligations under the *Contract."*

1.1.11 Insert a new paragraph 1.1.11 as follows:

"This *Contract* shall constitute the entire and only agreement between the parties relating to the subject matter hereof, superseding any previous agreements or understandings. There are no agreements, understandings, or covenants between the parties of any kind, expressed or implied, oral or otherwise, pertaining to the *Work* hereunder which have not been set forth or specified herein. This *Contract* cannot be modified except by an instrument in writing signed by an authorized representative of each party."

GC 1.4 ASSIGNMENT

1.4.1 Delete in its entirety and replace with:

Contractor shall not assign the Contract or a portion thereof without the written consent of *Owner*. *Owner* shall be permitted to assign the Contract to *Owner's* client upon notice to *Contractor*.

GC 2.4 DEFECTIVE WORK

2.4.1.1 Add new paragraphs 2.4.1.1 and 2.4.1.2 as follows:

"2.4.1.1 The *Contractor* shall rectify, in a manner acceptable to the *Owner*, all defective *Work* and deficiencies throughout the *Work*, whether or not they are specifically identified by the *Owner*.

"2.4.1.2 The *Contractor* shall prioritize the correction of any defective *Work* which, in the sole discretion of the *Owner*, adversely affects the day to day operation of the *Owner*."

GC 3.2 CONSTRUCTION BY OWNER OR OTHER CONTRACTOR

3.2.4 Amend paragraph 3.2.4 by adding the following language to the end of the paragraph:

"For other contractors and the *Owner's* own forces, the *Contractor* shall assume overall responsibility for compliance with OHSA and all other aspects of the applicable health and

safety legislation of the *Place of the Work*, including the responsibilities of the "constructor" under OHSA."

GC 3.5 CONSTRUCTION SCHEDULE

3.5.1.1 Delete "first application for payment" and replace with "commencement of *Work*"

GC 3.7 SUBCONTRACTORS AND SUPPLIERS

3.7.3 Delete paragraph 3.7.3 in its entirety and replace with the following language:

"3.7.3.1 All *Subcontractors* and *Suppliers* must be acceptable to *Owner* and its client, and *Owner* and its client reserve the right to require *Contractor* to remove immediately any *Subcontractor* or *Supplier* from performing the *Work*, with or without cause, in the *Owner*'s or its client's sole discretion for reasons including, but not limited to, substance abuse."

"3.7.3.2 Fusion Program. The *Owner* has a capital expenditure sourcing program ("Fusion Program") that utilizes the *Owner's* global, national and regional scale to drive cost reduction and savings by working with qualified service providers and suppliers ("Fusion Partners"). Additional benefits include speed to market, superior customer service, maximization of value management, innovation, and commitment. *Contractor* will, as part of its responsibilities hereunder, work with the Fusion Partners' representatives to obtain pricing and other value-add benefits. The *Owner* shall provide *Contractor* with the name and contact information for the Fusion Partners, as may be amended from time to time."

3.7.4 Add the following to the end of 3.7.4:

"Contractor shall provide Owner advance written notice and obtain Owner's advance written approval for any proposed Subcontract change order."

3.7.5 Add the following new paragraph:

"3.7.5 Contractor shall not enter into any subcontract with any affiliated entity unless such arrangement has been approved in writing by Owner."

GC 3.8 LABOUR AND PRODUCTS

3.8.2 Delete paragraph 3.8.2 in its entirety and replace with the following language:

"*Products* provided shall be new and shall conform to all current applicable specifications of the Canadian Standards Association, Canadian Standards Board or General Standards Board, ASTM, National Building Code, (based on the respective provincial legislation or authority having jurisdiction the "Building Code") and all governmental authorities having jurisdiction at the *Place of the Work*, unless otherwise specified. *Products* which are not specified shall be of a quality consistent with those specified and their use acceptable to the *Owner*. *Products* brought on to the *Place of the Work* by the *Contractor* shall be deemed to be the property of the *Owner*, but the *Owner* shall be under no liability for loss thereof or damage thereto arising from any cause whatsoever, and such *Products* shall be at the sole risk of the *Contractor*."

GC 3.10 SHOP DRAWINGS

3.10.13 Insert a new paragraph 3.10.13 as follows:

"Any and all *Shop Drawings* shall be the exclusive property of the *Owner* or the *Owner's* client as the case may be; and the *Contractor* hereby assigns all right, title and interest in the same to the *Owner* or the person or entity specifically directed by the *Owner*. Any and all *Shop Drawings* conceived by the *Contractor* prior to the term of this *Contract* and utilized by it in rendering duties to the *Owner* are hereby licensed to the *Owner* or the person or entity specifically directed by the *Owner* for use in its operations and for an infinite duration. This license may be assigned without *Contractor's* prior written approval by the *Owner* to the *Owner's* client, or to an affiliate or subsidiary of the *Owner*, or to its designee."

GC 3.14 STANDARD OF CARE

Add new General Condition 3.14 as follows:
"GC 3.14 STANDARD OF CARE

3.14.1 In performing the *Work* under the *Contract*, the *Contractor* shall exercise a standard of care, skill and diligence that would normally be provided by an experienced and prudent *Contractor* supplying similar services for similar projects. The *Contractor* acknowledges and agrees that throughout the *Contract*, the *Contractor's* obligations, duties and responsibilities shall be interpreted in accordance with this standard. The *Contractor* shall exercise the same standard of due care and diligence in respect of any *Products*, personnel, or procedures which it may recommend to the *Owner*.

3.14.2 The *Contractor* further represents, covenants and warrants to the *Owner* that:

.1 The personnel it assigns to the *Project* are appropriately experienced;

.2 It has a sufficient staff of qualified and competent personnel to replace its designated supervisor and project manager, subject to the *Owner's* approval, in the event of death, incapacity, removal or resignation; and

.3 There are no pending, threatened or anticipated claims that would have a material effect on the financial ability of the *Contractor* to perform its *Work* under the *Contract*."

GC 3.15 OCCUPANCY OF THE WORK

Add a new General Condition 3.15 as follows:
"GC 3.15 OCCUPANCY OF THE WORK:

3.15.1 The *Owner* reserves the right to take possession of and use for any intended purpose, including the placement of fittings and equipment, any portion or all of the undelivered portion of the *Project*, even though the *Work* may not have reached *Substantial Performance of the Work*, provided that such taking of possession and use will not interfere, in any material way, with the progress of the *Work*. The taking of possession or use of any such portion of the *Project* shall not be deemed to be the *Owner's*

acknowledgement or acceptance of the *Work* or *Project*, nor shall it relieve the *Contractor* of any of its obligations under the *Contract*.

3.15.2 Where the *Project* contemplates *Work* by way of renovations in buildings which will be in use or be occupied during the course of the *Work*, or where the *Project* involves *Work* that is adjacent to a structure which is in use or is occupied, the *Contractor*, without in any way limiting its responsibilities under this *Contract*, shall take all reasonable steps to avoid interference with fire exits, building access and egress, continuity of electric power and all other utilities, to suppress dust and noise, to avoid conditions likely to propagate mould or fungus of any kind, and all other steps reasonably necessary to promote and maintain the safety and comfort of the users and occupants of such structures or adjacent structures. Without *Owner's* prior approval, the *Contractor* shall not permit any Worker or *Subcontractors* to use any existing facilities including, without limitation, lavatories, toilets, entrances and parking areas other than those designated by the *Owner*."

GC 4.1 - CASH ALLOWANCES

4.1.4 Delete paragraph 4.1.4 in its entirety and substitute new paragraph 4.1.4:

"Where costs under a cash allowance exceed the amount of the allowance, unexpended amounts from other cash allowances shall be reallocated at the Consultant's direction to cover the shortfall."

4.1.5 Delete paragraph 4.1.5 in its entirety and substitute new paragraph 4.1.5:

"The unexpended total cash allowance amount shall be deducted from the Contract Price by Change Order."

4.1.8 Add new paragraph 4.1.8:

"4.1.8 The Owner reserves the right to call, or to have the Contractor call, competitive bids for portions of the Work, to be paid for from cash allowances."

GC 5.1 FINANCING INFORMATION REQUIRED OF THE OWNER

5.1.1 Delete 5.1.1 in its entirety.

5.1.2 Delete 5.1.2 in its entirety.

GC 5.2 APPLICATIONS FOR PROGRESS PAYMENTS

5.2.2 Insert the following at the end of 5.2.2:

"Each application for payment shall be certified by a duly authorized officer or principal of the *Contractor* and contain such additional information as *Owner* may reasonably request. All applications for payment shall be deemed a representation and warranty that the funds will be applied solely towards the items certified therein."

5.2.8 Insert a new paragraph 5.2.8 as follows:

"To the extent permitted by applicable law, with each application for payment, *Contractor* shall also submit (i) a fully-executed Statutory Declaration from *Contractor* (conditioned only upon payment of the amount in the application for payment) for all charges reflected in such application for payment, (ii) except with respect to the first application for payment, fully-executed unconditional lien waivers from all *Subcontractors* and *Suppliers* for all labor, materials and equipment provided under any prior application for payment for which the *Owner* has delivered payment to *Contractor*, and (iii) such additional information as the *Owner* may reasonably require."

GC 5.4 SUBSTANTIAL PERFORMANCE OF THE WORK

5.4.3 Delete paragraph 5.4.3 in its entirety and substitute new paragraph 5.4.3:

"Immediately following the issuance of the certificate of Substantial Performance of the Work, the Contractor, in consultation with the Consultant, shall establish reasonable dates for finishing the Work and correcting deficient Work."

5.4.4 Add new paragraph 5.4.4:

"The Contractor shall publish, in a construction trade newspaper in the area of the location of the Work, a copy of the Certificate of Substantial Performance of the Work within seven (7) days of receiving a copy of the Certificate signed by the Consultant, and the Contractor shall provide suitable evidence of the publication to the Consultant and Owner. If the Contractor fails to publish such notice, the Owner shall be at liberty to publish and back charge the Contractor its reasonable costs for doing so.

5.4.5 Add new paragraph 5.4.5:

Prior to submitting its application for Substantial Performance of the Work, the Contractor shall submit to the Consultant all:

.1 guarantees,

.2 warranties,

.3 certificates,

.4 testing and balancing reports,

.5 distribution system diagrams,

.6 spare parts,

.7 maintenance manuals,

.8 commissioning documents and manuals,

and other materials or documentation required to be submitted under the Contract, together with written proof acceptable to the Owner and the Consultant that the Work has been substantially performed in conformance with the requirements of municipal, government and utilities authorities having jurisdiction.

5.4.6 Add new paragraph 5.4.6:

Where the Contractor is unable to deliver the documents and materials described in paragraph 5.4.5, then, provided that none of the missing documents and materials interferes, in a material way, with the use and occupancy of the Work, failure to deliver shall not be grounds for the Consultant to refuse to certify Substantial Performance of the Work. Any documents or materials not delivered in accordance with paragraph 5.4.5 shall be delivered as provided in GC 5.7."

GC 5.5 PAYMENT OF HOLDBACK UPON SUBSTANTIAL PERFORMANCE OF THE WORK

5.5.1 Add new paragraphs 5.5.1.3, 5.5.1.4 and 5.5.1.5:

5.5.1.3 Submit a written request for release of holdback including a declaration that no written notices of lien have been received by it.

5.5.1.4 Submit a Statutory Declaration CCDC 9A-2001.

5.5.1.5 Submit WSB Clearance Certificate.

GC 5.7 FINAL PAYMENT

5.7.5 Insert a new paragraph 5.7.5 as follows:

"Acceptance of final payment by *Contractor*, a *Subcontractor*, or *Supplier* shall constitute a waiver of claims by the payee, except for those matters described in a written notice from such payee to the *Owner* delivered with or prior to the application for final payment, identifying any such matters that are unsettled at the time of application for final payment. Contractor shall cause all guarantees and warranties with respect to the Work to be assigned or be otherwise enforceable by Owner."

GC 6.2 CHANGE ORDER

6.2.3 Insert a new paragraph 6.2.3 as follows:

The value of a change shall be determined in one or more of the following methods as directed by the Owner:

.1 by estimate and acceptance of a lump sum.

.2 by unit prices established in the Contract or subsequently agreed upon. Unit prices shall include overhead, profit, and other reasonable charges of the Contractor and shall be the total cost to the Owner. Adjustment to the Contract Price shall be based on a net quantity difference from the original quantity.

.3 by actual credits and costs to the Owner. Where additional Work is required, the cost to the Owner shall be the actual cost plus the following percentage fee for overhead and profit, after all credits included in the change have been deducted. Permitted mark-ups for overhead and profit are:

(1) on Work performed by the Contractor's own forces, a maximum of 5% combined percentage for overhead and profit;

(2) on Work performed by Subcontractors, the Subcontractors may charge a maximum of 10% combined percentage for overhead and profit and the Contractor may charge a maximum of 5% combined percentage for overhead and profit on Work performed by Subcontractors.

6.2.4 Insert a new paragraph 6.2.4 as follows:

The mark-ups described in paragraph 6.2.3.3 include all necessary supervision, general account items, general clean-up, small tools, as-built drawings and job safety necessary to perform the change. Additional bonding cost is excluded from the mark-ups but may be included as a cost, using the value declared for bonding by the Contractor in its bid to the Owner, unless otherwise agreed by the parties."

GC 6.4 CONCEALED OR UNKNOWN CONDITIONS

Delete paragraph 6.4.1 in its entirety and replace it with the following:

"**6.4.1.1** The *Contractor* confirms that, prior to tendering for the *Project*, it fully investigated the *Place of the Work*. In that investigation, the *Contractor* applied the degree of care and skill described in paragraph 3.14.1. To the extent that such investigation permits, the *Contractor* has satisfied itself as to:

.1 the nature and location of the *Work*;
.2 the character and content of the *Work* to be done;
.3 the results and improvements once the *Work* is completed;
.4 the nature and confirmation of all conditions of the *Place of the Work*, including soil conditions and the location of any utility which might affect the *Work*;
.5 the character and content of the scope of the *Work* to be done by other contractors and the *Owner*;
.6 the proximity and special arrangement of all existing equipment and facilities which may affect the execution of the *Work*;
.7 the equipment and facilities needed for the on-time execution and completion of the *Work*;
.8 all labour restrictions including availability of skilled trades;
.9 safety hazards and labour contract negotiations which may have an impact on the execution of the *Work*;
.10 the location of any required utility or service;
.11 without limiting the generality of the foregoing, any condition or circumstance which may affect the conduct of the *Work*.

6.4.1.2 If the *Contractor* has not conducted such careful investigation, it is deemed to assume all risk of conditions or circumstances now existing or arising in the course of the *Work* which could make the *Work* more expensive or more difficult to perform than was contemplated at the time the *Contract* was executed. No claim by the *Contractor* will be entertained in connection with conditions which could reasonably have been ascertained by an investigation or other due diligence undertaken prior to execution of the *Contract*."

6.4.2 Amend paragraph 6.4.2 by adding a new first sentence which reads as follows:

"Having regard to paragraph 6.4.1, if the *Contractor* believes that the conditions of the *Place of the Work* differ materially from those reasonably anticipated, or differ materially from those indicated in the *Contract Documents*, or were concealed from discovery notwithstanding the conduct of the investigation described in paragraph 6.4.1, it shall notify the *Owner* and *Owner's Client* in writing no later than five (5) *Working Days* after the first observation of such conditions."

6.4.2 Amend the existing second sentence of paragraph 6.4.2, in the second line, following the word "materially", by adding the words "or were concealed from discovery notwithstanding the conduct of the investigation described in paragraph 6.4.1".

6.4.3 Delete paragraph 6.4.3 and replace with the following language:

"If the *Consultant* makes a finding pursuant to paragraph 6.4.2 that no change in the *Contract Price* or *Contract Time* is justified, the *Consultant* shall report in writing the reasons for this finding to the *Owner* and the *Contractor*."

GC 6.5 DELAYS

6.5.6 Insert a new paragraph 6.5.6 as follows:

"If *Contractor* is delayed in the performance of the *Work* by an act of omission of the *Contractor* or any of its *Subcontractors* or anyone employed or engaged by them directly or indirectly, then, notwithstanding any extension in the *Contract Time* that may be agreed to in writing, *Contractor* shall pay or cause to be paid to *Owner* any and all damages, including, but not limited to, liquidated damages, if any. *Owner* may deduct the same from payment due or to become due to *Contractor*."

GC 7.1 OWNER'S RIGHT TO PERFORM THE WORK, TERMINATE THE CONTRACTOR'S RIGHT TO CONTINUE WITH THE WORK OR TERMINATE THE CONTRACT

7.1.7 Insert a new paragraph 7.1.7 as follows:

"The *Owner* may terminate the *Contract* for convenience, either in whole or in part, without liability, fee, or penalty, at any time and without cause upon thirty (30) days prior written notice to the *Contractor*. On receipt of notice of termination for convenience, *Contractor* shall, unless the notice directs otherwise, immediately discontinue the *Work* and placing of orders for materials, equipment, and supplies in connection with the performance of the *Work*, and shall, if requested, make every reasonable effort to procure cancellation of all existing orders or contracts upon terms satisfactory to the *Owner*, and shall thereafter do only such *Work* as may be necessary to preserve and protect the *Work* already in progress and to protect material, plant and equipment or in transit thereto.

Upon a termination for convenience, *Contractor* shall be entitled only to pro-rata compensation for the portion of the *Work* already performed, including engineering and materials for which it has made firm contracts, it being understood that the *Owner* shall be entitled to such materials and drawings."

GC 7.2 CONTRACTOR'S RIGHT TO SUSPEND THE WORK OR TERMINATE THE CONTRACT

7.2.1 Delete 7.2.1 in its entirety.

7.2.2 Delete "20" and replace with "30"

7.2.2 Delete "terminate" and replace with "suspend"

7.2.4 Delete "or terminate the *Contract*"

7.2.5 Delete the paragraph in its entirety and replace with the following language:

"If *Contractor* suspends the *Contract* under the conditions set out above, the *Contractor* shall be entitled only to pro-rata compensation for the portion of the *Work* already performed, including engineering and materials for which it has made firm contracts, it being understood that the *Owner* shall be entitled to such materials and drawings. Should *Contractor's* suspension be a direct result of *Owner's* material default of its obligations under the *Contract*, and such suspension continues for longer than sixty (60) *Working Days*, the *Contractor* and the *Owner* may, through the *Change Order* process, agree to an equitable adjustment in the *Contract Price*."

GC 8.2 NEGOTIATION, MEDIATION AND ARBITRATION

8.2.7 Delete the paragraph in its entirety and replace with the following language:

"The findings and determination through arbitration shall be final and binding on the parties."

GC 9.2 TOXIC AND HAZARDOUS SUBSTANCES

9.2.5.3 Delete 9.2.5.3 in its entirety and replace with the following language:

"stop performance on the *Work* immediately in the affected area and"…

9.2.6 Delete paragraph 9.2.6 in its entirety and replace with the following language:

"The *Owner* shall verify the presence or absence of the suspected toxic or hazardous substances or materials at the *Place of Work*, and, if present, verify that the toxic or hazardous substances or materials shall be remediated in accordance with applicable laws. After any toxic or hazardous substances or materials at the *Place of Work* have been remediated, the *Work* in the affected area shall resume. If the presence of toxic or hazardous substances or materials is not the result of the act or omissions of the *Contractor* or any of its *Subcontractors* or *Suppliers* or any other party for which the *Contractor* is responsible, then the *Contract Time* may be reasonably extended pursuant to a *Change Order*."

9.2.7.2 Add "and" after ";"

9.2.7.3 Delete "; and" and replace with "."

9.2.7.4 Delete 9.2.7.4 in its entirety.

9.2.8.2 Add “and” after “;”

9.2.8.3 Delete “; and” and replace with “.”

9.2.8.4 Delete 9.2.8.4 in its entirety.

9.2.9 Delete paragraph 9.2.9 in its entirety and replace with the following language:

“*Contractor* shall not transport to, use, generate, dispose of, or install at the *Place of Work* any toxic or hazardous substances or materials, except in accordance with applicable environmental laws and as expressly required under the *Contract Documents* and made known in advance and approved by the *Owner* in writing. *Contractor* shall not transport to, use, generate, dispose of, or install at the *Place of Work* any asbestos-containing material, even if such asbestos-containing material is not specifically banned under any environmental law. *Contractor* shall not cause any release of toxic or hazardous substances or materials into, or contamination of, the environment, including without limitation the soil, the atmosphere, any water course or ground water. To the fullest extent permitted by law, *Contractor* shall indemnify, defend (promptly and diligently, at *Contractor’s* sole expense with attorneys satisfactory to the Owner), and hold harmless the Indemnified Parties (as such term is defined below) against any and all damages, losses, liabilities, costs and expenses, including without limitation reasonable attorneys’ fees, liens, claims, demands and causes of action of every kind and character based upon, arising out of or resulting from *Contractor*, a *Subcontractor, Supplier* any of their direct or indirect agents or employees, or anyone for whose acts they may be liable in the performance of the *Work* engaging in the activities prohibited in this paragraph 9.2.9.

.”

GC 9.4 CONSTRUCTION SAFETY

Delete paragraph 9.4.1 in its entirety and replace with the following language:

"**9.4.1** The *Contractor* and not the *Owner* shall, for the duration of the *Project*, be solely responsible, and have overall responsibility, for construction health and safety at the *Place of the Work* and for compliance with the codes, laws, ordinances, rules, regulations and practices (collectively, “Codes”) which relate to construction health and safety and shall be responsible for initiating, maintaining, enforcing and supervising all health and safety precautions and programs in connection with the performance of the *Work* and the other work performed by *Owner* and *Owner’s* other contractors (“*Owner’s* Other Contractors”) at the *Place of the Work* (collectively, the “Other Work”), until *Total Performance* of the *Work*. The *Contractor* shall erect and maintain, as required by the *Owner’s* insurer, acting reasonably, code, and ordinance or by existing conditions and progress of the *Work*, safeguards necessary for health, safety and protection, including providing barriers, safety nets, scaffolding, barricades, fences, flagmen, fire prevention equipment and other measures, posting danger signs and other warnings against hazards, promulgating safety regulations and notifying owners and users of adjacent utilities and properties. *Owner* shall not direct or monitor or enforce safety at the *Place of Work*. *Owner’s* attendance at the *Place of Work* shall be for the purpose of monitoring progress and not for purposes of supervising, managing, scheduling or enforcing safety. The *Contractor* shall supervise and implement compliance of such health and safety requirements by:

.1 *Owner* and *Owner's* other contractors during the performance of Other Work by *Owner* and *Owner's* other contractors; and

.2 The *Subcontractors, Suppliers* and *Sub-subcontractors* during their performance of the *Work*.

9.4.2 Add a new paragraph 9.4.2 as follows:

"The *Contractor*, before commencement of any part of the *Work*, shall give any notices required to be given to the *Owner's* property manager, tenants or adjoining landowners and other parties."

9.4.3 Add a new paragraph 9.4.3 as follows:

Without restricting the generality of any other provision in the *Contract Documents*, for the duration of the *Project*, until *Total Performance of the Work*, the *Contractor* is the *Constructor* and the *Contractor* undertakes to carry out the duties and responsibilities of the Constructor with respect to the *Project* (including the *Work* of the *Subcontractors* and the work of contractors engaged by the Owner under separate contract) including the following:

.1 undertake the *Project* for the *Owner* pursuant to the health and safety requirements of OHSA and to carry out the measures and procedures prescribed by OHSA for the *Project*;

.2 ensure that every employer and worker at the *Project* complies with OHSA and receives appropriate health and safety instruction and training;

.3 protect the health and safety of workers on the *Project*;

.4 prepare and implement an overall work safety program and review the safety programs of each of the *Subcontractors* and any other contractors at the *Place of the* Work and enforce compliance at the *Place of the Work* by *Subcontractors* with such work safety program;

.5 as applicable in the jurisdiction of the *Place of the Work* file the *Notice of Project*, naming itself as *Constructor*, and file all other applicable registrations required by OHSA (including Section 5 of the construction regulations);

.6 report to the *Owner* and the *Consultant* all health and safety incidents at the *Place of the Work* that the *Contractor* becomes aware of, including the *Contractor's* response to such incidents; and

.7 inform all *Subcontractors* and all other contractors or persons at the *Place of the Work* of the *Contractor's* safety program and require *Contractor's Subcontractors* to have their own safety programs including established training programs that at a minimum meet *Contractor's* safety programs and training programs. The *Contractor* shall review such safety programs for compliance with *Contractor's* safety programs.

.8 provide timely notice of any unsafe work to any *Subcontractor, Supplier,* sub-subcontractor, *Owner* or *Owner's* other contractors or any other contractor or person on the *Place of the Work* and the *Contractor* shall stop the unsafe work and instruct them to cure the condition and shall order the immediate removal of any non-complying person from the *Place of the Work*.

.9 retain a properly trained and knowledgeable and competent person, as required by OHSA, in a supervisory position, to be responsible for initiating, maintaining and enforcing the *Contractor's* health and safety program at the *Place of the Work*, inspecting the *Place of the Work* and enforcing all applicable health and safety laws and regulations on the *Place of the Work*.

9.4.4 Add a new paragraph 9.4.4 as follows:

"The *Contractor* shall indemnify and hold harmless the *Owner* from any liability for claims, damages or penalties, including legal fees and costs to defend any offences, arising from the *Contractor's* failure to comply with the duties, responsibilities and obligations of the *Constructor* and employer under OHSA."

GC 10.2 LAWS, NOTICES, PERMITS, AND FEES

10.2.4 Insert the following at the end of this section:

"Contractor shall comply with the CBRE Supplier Code of Conduct located at http://www.cbre.com/suppliers and made a part hereof. Contractor shall comply with policies of Client and landlord provided to Contractor."

GC 10.3 PATENT FEES

10.3.1 Insert "and *Owner's* client" before "harmless"

10.3.2 Delete paragraph 10.3.2 in its entirety.

GC 11.1 INSURANCE

11.1.1. Insert the following in CCDC 41:

8. Workplace Safety and Insurance. *Contractor* shall provide a certificate of clearance from the applicable provincial workplace safety and insurance organization as evidence of compliance with all requirements of the applicable legislation, including payments due thereunder. *Contractor* shall provide such certificates on each anniversary date of the Agreement during the Term or whenever requested by *Owner* from time to time;

9. Employer's Liability. Coverage 'B' Employer's Liability with limits of at least $1,000,000 per accident per employee; $1,000,000 per disease per employee; and $1,000,000 per disease policy limit;

10. Umbrella Liability. Such insurance shall follow form on concurrent terms with and provide coverage with limits of not less than $5,000,000 per occurrence and $5,000,000 in the aggregate per property or location in excess of the underlying coverages

listed in clauses 1, 2, and 4 above having coverage which are at least as broad as the primary insurance coverage and the terms of the primary liability and excess (umbrella) liability policies are concurrent;

11. Errors and Omissions. **If the Work includes brokerage, architectural, design, engineering or other professional consulting services**, then *Contractor* shall obtain and maintain Professional Liability (E&O) insurance providing limits of not less than $1,000,000 per occurrence or such greater limit as *Owner* or Client may deem appropriate for the scope and nature of the Work provided. The coverage shall be continued by renewal or extended reporting provision for not less than three (3) years after completion of the Work; and

12. All Risk Builder's Risk Insurance. Except to the extent coverage is provided by Client, *Contractor* shall provide a standard builder's "all risk" insurance policy, subject to the exclusions contained therein and subject to a deductible that shall not exceed $10,000, in the name of *Owner*, Client and *Contractor* including the interest of *Contractor* on (a) the work that is done; and (b) all insurable items of work and materials to be incorporated in the work, title to which has been acquired by *Owner*, but such insurance shall not cover any property owned, leased or otherwise used in connection with the work by *Contractor* or its subcontractors. *Contractor* shall be responsible for the first $10,000 of any loss covered by the Builder's Risk Insurance policy.

11.1.9 Add the following:

11.1.9 Insurance Requirements.

11.1.9.1 License/Rating. All insurance policies shall be in customary forms and shall be issued by companies authorized to do business in the states where the services are performed and rated "A-," FSC Class VIII or better by the most current A. M. Best's Insurance Reports.

11.1.9.2 Certificate of Insurance. *Contractor* acknowledges and agrees that it shall deliver certificates of insurance evidencing the required insurance coverage to Owner and the client prior to the commencement of performance under any *Work* under this Agreement or upon any renewal of such insurance during the term of this Agreement not less than thirty (30) days prior to the expiration dates of any policy shown on the certificates then in effect, and otherwise from time to time upon request by the *Owner* or its client.

11.1.9.3 Notice of Cancellation. The *Owner* shall, be given not less than thirty (30) days' notice prior to the cancellation of any insurance required by this Agreement for other than non-payment of premiums. The *Owner* shall be given at least ten (10) days' notice prior to cancellation of any required insurance for non-payment of premium.

11.1.9.4 Vendor Screening/Certificate of Insurance. *Contractor* acknowledges and agrees that it will enroll, at *Contractor*'s sole expense, in the CBRE vendor screening and certificate of insurance management program. Registration in the CBRE vendor screening program can be completed on the internet at http://screening.cbre.com/canada

11.1.9.5 Additional Insured Endorsements. All certificates of insurance provided under this Agreement shall include copies of endorsements to *Contractor's* commercial general liability, workers compensation and automobile policies that include *Owner* and the client (including all participating affiliates) as additional insured(s) on appropriate ISO forms or equivalent form of Blanket Additional Insured Endorsement, covering the additional

insureds for liability arising from all operations and completed operations of the *Contractor*.

11.1.9.6 No Waiver/Deductible. The failure of the *Owner* to demand such certificate of insurance or failure of the *Owner* to identify a deficiency will not be construed as a waiver of the *Contractor's* obligation to maintain the insurance required under this Agreement. The *Contractor* shall be responsible for the amount of any deductible contained in any of the above-described insurance policies and certificates of insurance.

11.1.9.7 *Contractor* Insurance Primary. The *Contractor's* insurance shall be deemed primary with respect to coverage extended to the additional insureds, whose insurance shall be excess and non-contributory with that required of the *Contractor* hereunder.

11.1.9.8 Waiver of Subrogation. To the fullest extent permitted by law, all insurance policies shall contain provisions that the insurance companies waive the rights of recovery or subrogation against *Owner*, the client, their respective affiliates, and each of their and their affiliates' respective agents, officers, directors, shareholders, employees, insurers, successors and assigns.

11.1.9.10 Additional *Owner* Rights. The failure to secure and maintain or add by endorsement the Indemnified Parties shall not act as a defense to the enforcement of the terms of this Agreement. Any failure to provide the agreed endorsements shall entitle the *Owner* to terminate this Agreement or to acquire coverage necessary to protect *Owner* and the client from the failure and charge the cost thereof to the *Contractor*. The *Contractor* shall require or provide the same minimum insurance requirements as listed above from all of its permitted *Consultants* and subcontractors unless otherwise agreed by the *Owner* in writing.

GC 12.1 INDEMNIFICATION

12.1.1 Delete paragraph 12.1.1 and replace with the following:

"The *Contractor* shall indemnify, defend (promptly and diligently, at *Contractor*'s sole expense with attorneys satisfactory to the *Owner*), and hold harmless the *Owner*, *Owner's* client, *Consultant*, and each of their affiliates; respective agents, officers, directors, shareholders, contractors, insurers employees, subcontractors, successors and assigns (collectively, the "Indemnified Parties" and individually, an "Indemnified Party") from and against any liabilities, damages (including without limitation direct, special, and consequential damages), costs, expenses, suits, losses, claims, actions, fines, and penalties (including without limitation court costs, reasonable attorneys' fees, and any other reasonable costs of litigation) (hereinafter collectively, "Claims") that any of the Indemnified Parties may suffer, sustain, or incur as a result of or in connection with:

.1 *Contractor's Work* or presence at the *Place of Work* or other work site;

.2 any negligent acts, errors, or omissions, intentional misconduct, or fraud of *Contractor*, its employees, *Subcontractors, Suppliers,* or agents, whether active or passive, actual or alleged, whether in the provision of the Work, failure to provide any or all of the Work, or otherwise;

3. any breach of the *Contract Documents* by *Contractor* or its *Subcontractors* or *Suppliers*;

.4 assertions under workers' compensation or similar employee benefit acts by *Contractor* or its employees or agents, and/or any failure by *Contractor* to pay any employment benefits and any taxes required of it of any nature whatsoever;

.5 failure to comply with any applicable law by *Contractor*, *Subcontractor* or *Supplier*;

.6 claims by any *Subcontractor* or *Supplier* or employees of *Contractor's Subcontractors,* including, without limitation, for bodily injury or wrongful discharge; and/or

.7 any infringement or alleged infringement of any patent, copyright, trade secret, or other proprietary right of any third party relating to the *Work* performed under the *Contract Documents*.

The foregoing indemnification shall apply irrespective of whether Claims are asserted by an Indemnified Party, by its employees, agents, or subcontractors, or by unrelated third parties. Nothing contained herein shall relieve *Contractor* of any responsibility for Claims regardless of whether *Contractor* is required to provide insurance covering such Claims or whether the matter giving rise to the Claims is the responsibility of *Contractor*'s agents, employees or *Subcontractors,* or *Suppliers*. The provisions of this Section shall survive the termination of this Agreement."

12.1.2 Delete paragraph 12.1.2 in its entirety and replace with "Intentionally Omitted."

12.1.3 Delete paragraph 12.1.3 in its entirety and replace with "Intentionally Omitted."

12.1.7 Insert a new paragraph 12.1.7 as follows:

"In no event shall *Owner, Owner's* client or *Consultant* or any of their respective Indemnified Parties*,* be liable to *Contractor* for any lost or prospective profits or any special, punitive, exemplary, consequential, incidental, or indirect loss or damage, whether based in contract, warranty, indemnity, negligence, strict liability or other tort or otherwise, under or with respect to the *Contract Documents* or from any failure or performance related thereto, regardless of cause, even if advised of the possibility of such damages in advance and even if a remedy set forth herein is found to have failed of its essential purpose. "

GC 12.2 WAIVER OF CLAIMS

12.2.1 Delete "date of *Substantial Performance of the Work*" and replace with "receipt of final payment by the *Contractor,"*

12.2.2 Delete "date of *Substantial Performance of the Work*" and replace with "receipt of final payment by the *Contractor,"*

12.2.3 Delete paragraph 12.2.3 in its entirety and replace with "Intentionally Omitted."

12.2.4 Delete paragraph 12.2.4 in its entirety and replace with "Intentionally Omitted."

12.2.5 Delete paragraph 12.2.5 in its entirety and replace with "Intentionally Omitted."

12.2.8 Delete "or 12.2.3"

12.2.9 Delete paragraph 12.2.9 in its entirety and replace with "Intentionally Omitted."

12.2.10 Delete paragraph 12.2.10 in its entirety and replace with "Intentionally Omitted."

GC 12.3 WARRANTY

12.3.1 Delete "date of *Substantial Performance of the Work*" and replace with "receipt of final payment by the *Contractor*"

12.3.2 Add the following language to paragraph 12.3.2:

"The materials and equipment used or furnished in connection with the *Work* shall be of first class quality, new in all respects and not used, reworked, refurbished, or rebuilt, unless otherwise approved by the *Owner*, and *Contractor* shall, where applicable, deliver clear title to equipment, materials, and improvements provided under the *Contract Documents. Contractor* shall provide proof that all materials and equipment provided as part of the *Work* are free from all encumbrances. If there is a breach of the foregoing warranty, the *Contractor*, in the *Owner's* sole discretion and at *Contractor's* sole cost and expense, shall promptly repair or cause to be repaired any such defects in the *Work*."

12.3.4 Add the following language to paragraph 12.3.4:

"If the *Owner* elects to repair the defect on its own, it may do so in its sole discretion without any notice to *Contractor*, and *Contractor* shall nevertheless be responsible for any and all costs and expenses incurred by the *Owner*."

12.3.7 Add a new subsection 12.3.7 as follows:

"The warranties set out in this GC 12.3 -- WARRANTY are not exclusive of any other warranties or guarantees set out in the *Contract Documents* or available under applicable law. The warranties of *Contractor* and *Subcontractors* provided in this paragraph shall in no way limit or abridge the warranties of the *Suppliers* of materials, equipment, and systems which are to comprise a portion of the *Work*. *Contractor* shall not act or fail to act in any way which results in the termination, expiration, or modification of such third party warranties or which otherwise results in prejudice to the rights of the *Owner* or *Owner's* client under such warranties."

Add a new GC 13 CONFIDENTIALITY

GC 13 CONFIDENTIALITY

13.1.1 Confidentiality Obligations. All Confidential Information owned by the Disclosing Party is and shall remain the property of such party at all times. By disclosing Confidential Information to the Receiving Party, the Disclosing Party does not grant any express or implied licenses to the Receiving Party in any proprietary rights, including without limitation, patents, copyrights, trademarks, trade secret or trade secret information of the Disclosing Party, except as expressly stated in this Agreement or a Statement of Work issued hereunder. As of the Effective Date, the Confidentiality terms of this Agreement shall supersede and replace the terms of any Confidentiality or Non-Disclosure Agreement previously executed by the Parties with respect to subject matter that is covered by this Agreement. The Receiving Party agrees to utilize the Confidential Information received by it only for the purpose of fulfilling the purpose of this Agreement and for no other purpose whatsoever, including, with respect to Contractor, without limitation, diverting, inducing or attempting to divert or induce *Client* to discontinue or modify the present or future relationship between *Owner* and *Client*, or otherwise injuring or interfering in the business relationship between *Owner* and *Client*. The Receiving Party shall use the same care and discretion to avoid disclosure, publication or dissemination of any Confidential Information received from the Disclosing Party as the Receiving Party uses with its own confidential information that it does not wish to disclose, publish or disseminate, but in no event less than a reasonable degree of care. The Receiving Party shall not disclose

to any person (other than as necessary to agents and employees with a need to know about the same to achieve the purpose of this Agreement) Confidential Information at any time, either during the Term or at any time thereafter, without the express written agreement of Disclosing Party. The Receiving Party shall advise all recipients of Confidential Information as to the provisions of this Section and obtain their written agreement to be bound by its conditions. Notwithstanding the foregoing restrictions on the disclosure of Confidential Information, when *Owner* is the Receiving Party of Contractor Confidential Information, *Owner* may disclose Contractor Confidential Information with the applicable *Client* without restriction which disclosure shall not be deemed to be a violation of this Section. Upon the termination of this Agreement, the Receiving Party shall immediately deliver to the Disclosing Party upon request (i) any and all materials provided to the Receiving Party, relating in any way to and/or created in connection with the performance of this Agreement under the terms of this Agreement; and (ii) any and all originals, copies, reproductions and summaries (including without limitation, any written or electronic form of any such information) of any Confidential Information, or at Disclosing Party's option, certify destruction of the same. The Receiving Party shall incorporate the requirements of this Section in all subcontracts, requiring each approved subcontractor to comply with the provisions hereof in the same manner as is required of Receiving Party. Receiving Party shall immediately report to Disclosing Party any unauthorized disclosure of Confidential Information.

13.1.2 Confidential Information Exclusions. The Receiving Party shall not be liable for disclosure or use of any Confidential Information if: (i) it was in the public domain at the time it was disclosed or used through no fault of the Receiving Party; (ii) it becomes known to the Receiving Party from a source other than the Disclosing Party without a breach of this Agreement by the Receiving Party; (iii) it was independently developed by the Receiving Party without the benefit of the information received from the Disclosing Party; or (iv) it was disclosed under legal process or other legal requirement provided the Receiving Party agrees to cooperate in seeking reasonable protective arrangements requested by the Disclosing Party, and to promptly notify the Disclosing Party if the Receiving Party receives any subpoena or other legal process seeking disclosure of Confidential Information.

Add new GC 14 RECORDS; AUDIT

GC 14 RECORDS; AUDIT

14.1.1 Records. *Contractor* shall retain and maintain accurate records and documents relating to performance of Work under this Agreement until: (a) three (3) years after the termination or expiration of this Agreement unless a longer period is legally required; (b) the final resolution of all audits; (c) the conclusion of any litigation with respect to this Agreement; or (d) such longer time period as may be required by *Client's* record retention policy, whichever of subsections (a) through (d) is longer.

14.1.2 Audit. *Owner* or *Client* and/or an auditor designated by *Owner* or *Client* will have the right, at all reasonable times, and with not less than seven (7) business days prior notice to Contractor, to conduct financial, operational and technical audits of *Contractor* and its subcontractors to verify compliance with the terms and conditions of this Agreement, the accuracy of the charges invoiced by Contractor (and its subcontractors) and *Contractor's* performance of the Work. In addition, any governmental authority with jurisdiction over *Client* will have the right to audit *Contractor* to the extent that such governmental authority could have audited *Client* if *Client* were performing the *Work* internally. *Owner* and *Client* will have the right to audit *Contractor's* (and its subcontractors') processes, procedures, operations and performance for *Client's* operational risk assessment, regulatory requirements and annual reporting. *Owner's* and *Client's* right to audit extends to internal and external auditors, inspectors, regulators, and other representatives designated by *Owner* and *Client* (including customers, suppliers and other third parties to the extent *Owner* and *Client* are legally or contractually obligated to submit to audits by such entities). *Contractor* shall provide access to *Contractor's* books and records relating to the Work and such cooperation and assistance

as may be reasonably requested by *Owner*, *Client* or any auditor in connection with any audit required hereunder. *Contractor* shall promptly remedy any deficiencies revealed by any such audit without charge to *Owner* or Client. Any amounts determined to have been charged by Contractor incorrectly or for non-conforming Work shall be refunded by *Contractor* immediately without additional cost to *Owner* or Client. This Section shall survive the expiration or termination of this Agreement.

Add new GC 15 RESTRICTIONS ON USE OF NAME AND MARKS

GC 15 RESTRICTIONS ON USE OF NAME AND MARKS. *Contractor* shall not use or display *Owner's* or *Client's* name or logo and shall not utilize other trademarks or service marks of *Owner* or *Client*, without such party's prior written consent. Neither *Contractor* nor its agents or subcontractors may issue any press, media or publicity releases or give statements to the media identifying *Owner* or *Client* or relating to this Agreement or any Facility without the prior written consent of *Owner*.

Add **Schedule B Client Required Flow Down Provisions**
(attached as applicable)

DATED as of the ___ day of _____, _____.

OWNER: CBRE LIMITED

Per: _____
Name:
Title:

I/We have authority to bind the Corporation.

CONTRACTOR:

Per: _____
Name:
Title:

I have authority to bind the Corporation.