File No.: 2026-240

June 19, 2026

s.22(1)

Dear s.22(1)

Re: **Request for Access to Records under the Freedom of Information and Protection of Privacy Act (the "Act")**

I am writing regarding your request dated March 27, 2026 under the ***Freedom of Information and Protection of Privacy Act*** for:

1. **The most current contract/agreement (and appendices/amendments) related to the 450 (or 451) Beach Crescent public EV charging stations;**
2. **Any incident reports about the cutting or stealing of those charging cables and records about decisions to repair/replace cut chargers. Only inclusive of City or vendor reports (not a record of every single member of the public reporting cut cables); and**
3. **Record of any contracts that specify an obligation to maintain or repair the EV chargers.**

Date range: January 1, 2021 to March 26, 2026. Note: If the current contracts are dated prior to 2021 and are still in effect, please provide.

All responsive records are attached. Some information in the records has been severed (blacked out) under s.15(1), s.15(1)(l), and s.22(1) of the Act. You can read or download these sections here: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_00.

Please note, Electrical Design staff have advised our office that the City is actively investigating anti-theft solutions for the Public EV Fleet. If you wish to inquire further, please contact Jason Bethell, Business Support Manager, at jason.bethell@vancouver.ca.

*Please note, due to the file size of the responsive records package it has been uploaded to a City of Vancouver secured SharePoint site. Access details can be located in the email received alongside this letter.

Under Part 5 of the Act, you may ask the Information & Privacy Commissioner to review any matter related to the City's response to your FOI request by writing to: Office of the Information

& Privacy Commissioner, info@oipc.bc.ca or by phoning 250-387-5629.

If you request a review, please provide the Commissioner's office with: 1) the request number (2026-240); 2) a copy of this letter; 3) a copy of your original request; and 4) detailed reasons why you are seeking the review.
Yours truly,

Kevin Tuerlings, FOI Case Manager, for

[Signed by Kevin Tuerlings]

Siân Madsen, MA, MAS
Acting Director, Access to Information & Privacy

If you have any questions, please email us at foi@vancouver.ca and we will respond to you as soon as possible. You may also contact 3-1-1 (604-873-7000) if you require accommodation or do not have access to email.

Encl. via transfer site (Response Package)

:ma

TERMINATION AGREEMENT

THIS TERMINATION AGREEMENT made as of August 12,2025.

BETWEEN:

ZECO SYSTEMS CANADA INC. dba SHELL RECHARGE SOLUTIONS ("SRS")

ZECO HOLDINGS, INC.
("Zeco Holdings")

ZECO SYSTEMS, INC.
("Zeco Systems" and, together with Zeco Holdings, the "SRS Guarantors" and collectively with SRS, "Shell")

AND

CITY OF VANCOUVER
("Vancouver")

(individually a "**Party**" and collectively the "**Parties**")

BACKGROUND:

A. The Parties entered into two supply agreements (together, including all amendments, addendums, schedules and appendices, the "**Supply Agreements**"):

   a. SUPPLY AGREEMENT RELATING TO SUPPLY OF EV CHARGING EQUIPMENT AND SERVICES – RFP PS20180339 dated 22 June 2021 under which Vancouver, as a municipal corporation, would procure electric vehicle charging goods and services from SRS (the "**Public Agreement**").

   b. SUPPLY AGREEMENT RELATING TO PS20210275 – PROVISION OF CITY FLEET ELECTRIC VEHICLE CHARGING INFRASTRUCTURE, MAINTENANCE, AND SUPPORT dated 27 November 2023 under which Vancouver, as a municipal corporation, would procure electric vehicle charging goods and services from SRS with respect to Vancouver's fleet of electric vehicles (the "**Fleet Agreement**").

B. SRS notified Vancouver via Customer Notification Letter dated 12 December 2024 and email that it intended to end its Shell Sky software and Shell Sky software support of non-company-owned electric vehicle (EV) chargers in the US and Canada by no later than 30 April 2025, and that SRS would work with Vancouver to manage the transition including by discussing the remaining obligations SRS has under the Supply Agreements.

C. The Parties now wish to terminate the Supply Agreements on the terms set and conditions set out in this Termination Agreement.

NOW THEREFORE, the Parties agree as follows:

1. Interpretation

1.1. Any capitalized terms contained in this Termination Agreement that are not otherwise defined herein have the meaning set out in the relevant Supply Agreement.

1.2. In this Termination Agreement, including the Background, in addition to the terms otherwise specifically defined, the following terms have the following meanings:

a) "**Affiliate**" means with respect to any Person, any other Person directly or indirectly controlling, controlled by or under direct or indirect common control of such Person. A Person shall be deemed to control another Person if such Person possesses, directly or indirectly, the power to direct or determine the direction of the management and policies of other Person, whether through ownership of voting securities, by contract or otherwise.

b) "**Claims**" means any actions, causes of action, claims, suits, damages, losses, expenses, debts, dues, costs, interest, duties, obligations, covenants, representations, warranties, liabilities, and demands of any and every kind and nature whatsoever, at law, in equity or under any statute.

c) "**Vancouver Releasees**" means Vancouver, its Affiliates and partners, and all of their respective current and former elected officials, directors, officers, employees, agents, insurers, representatives and professional advisors including lawyers, accountants, consultants, and financial advisors, and each of their respective heirs and successors.

d) "**Person**" means any individual, corporation, firm, body corporate, trust, partnership, joint venture, government, governmental body, association, unincorporated organization or any other legal entity.

e) "**Shell Privacy Obligations**" means the obligations of a Shell Party, as applicable, under (i) Applicable Privacy Laws, Section 15.1 and Schedule E of the Public Agreement and (ii) Section 15.1 of the Fleet Agreement,

f) "**Shell Releasees**" means Shell, its Affiliates and partners, and all of their respective current and former directors, officers, employees, agents, insurers, representatives and professional advisors including lawyers, accountants, consultants, and financial advisors and each of their respective heirs and successors.

2. Termination

2.1. The Supply Agreements are hereby terminated as of 30 April 2025 (the "**Termination Date**"). From and after the Termination Date, the Supply Agreements will be of no further force or effect, and the rights and obligations of each of the Parties thereunder shall terminate.

2.2. Notwithstanding the termination of the Supply Agreements, SRS will, and the SRS Guarantors will cause SRS to comply with the following covenants provided such covenants will expire on the second anniversary of the date of this Termination Agreement:

a) comply with the SRS obligations on termination set out in Section 12.4(a) of the Public Agreement and Section 12.4(a) of the Fleet Agreement to the extent any are applicable and have not already been complied with by SRS on the date of this Termination Agreement; and

b) if required by Vancouver, assign all third party product and service warranties under the Supply Agreement to Vancouver.

2.3. Shell (a) is not aware, as of the date of this Termination Agreement, of any breach of the Shell Privacy Obligations, and (b) covenants that if after the Termination Date Shell still has access to "personal information" (as such term (or equivalent) is defined in Applicable Privacy Laws, the *Freedom of Information and Protection of Privacy Act* (British Columbia) or the *Personal Information Protection Act* (British Columbia) obtained by Shell under the Supply Agreements, Shell will continue to comply with the Shell Privacy Obligations.

3. Termination Payment

3.1. As consideration for the obligations, agreements and undertakings of the Parties under this Termination Agreement, SRS agrees to pay Vancouver a lump sum of CAD 106,123.78 (the "**Termination Payment**") which represents (i) a write-off of all outstanding invoices owed by Vancouver to SRS, (ii) a cash payment for services prepaid by Vancouver but not yet delivered, and (iii) amounts claimed by Vancouver as a consequence of SRS ceasing to provide the services set out in the Supply Agreements. The table included in Appendix A – Payment Breakdown provides further details.

3.2. No later than 45 days after the date of this Termination Agreement, Shell shall pay the Termination Payment to Vancouver via electronic funds transfer.

4. Mutual Release

4.1. Subject to (a) Shell complying with the terms of this Termination Agreement, (b) Vancouver receiving the Termination Payment in accordance with the terms of this Termination Agreement, and (c) any and all existing and future Vancouver Claims that Vancouver may make against the Shell Releases (provided Vancouver makes such Claims before the third anniversary of the date of this Termination Agreement) in any way arising from or related to a breach by Shell of any prior, existing or future Shell Privacy Obligations being expressly excluded from the scope of the Vancouver release under this section 4.1, Vancouver hereby forever releases the Shell Releasees of and from any and all existing and future Claims which Vancouver ever had, now has or may hereafter have, whether known or undiscovered, against the Shell Releasees in any way arising from or related to the Supply Agreements.

4.2. Subject to Vancouver complying with the terms of this Termination Agreement, Shell hereby forever releases the Vancouver Releasees of and from any and all existing and future Claims which Shell ever had, now has or may hereafter have, whether known or undiscovered, against the Vancouver Releasees in any way arising from or related to the Supply Agreements.

5. Representations and Warranties

5.1. Each Party hereby represents and warrants to the other Party that:

a) It has the full right, power and authority to enter into this Termination Agreement and to perform its obligations hereunder.

b) The execution of this Termination Agreement by the individual whose signature is set forth at the end of this Termination Agreement on behalf of such Party, and the delivery of this Termination Agreement by such Party, have been duly authorized by all necessary corporate action on the part of such Party.

c) This Termination Agreement has been executed and delivered by such Party and (assuming due authorization, execution, and delivery by the other Party hereto) constitutes the legal, valid, and binding obligation of such Party, enforceable against such Party in accordance with its terms.

d) It (i) knows of no Claims against the other Party relating to or arising out of the Supply Agreements that are not covered by the mutual release contained in Section 4, and (ii) has neither assigned nor transferred any of the Claims released herein to any Person and no Person has subrogated to or has any interest or rights in any Claims.

5.2. EACH PARTY HERETO ACKNOWLEDGES THAT, IN ENTERING INTO THIS TERMINATION AGREEMENT, IT HAS NOT RELIED UPON ANY REPRESENTATION OR WARRANTY MADE BY THE OTHER PARTY, OR ANY OTHER PERSON ON SUCH OTHER PARTY'S BEHALF, EXCEPT AS SPECIFICALLY PROVIDED IN THIS SECTION 5.

6. Confidentiality

6.1. The Parties shall maintain the terms and existence of this Termination Agreement in confidence subject only to such disclosure as may be required, in respect of Vancouver, by Vancouver City Council in accordance with the terms of the *Vancouver Charter* (British Columbia), and in respect of Vancouver and Shell, by law, by order of a court of competent jurisdiction, for purposes of securities, financial or tax reporting, or as otherwise required to give effect to this Termination Agreement.

7. No Admission of Liability

7.1. Nothing in this Termination Agreement is intended to be an admission of any liability by either Party.

8. General

8.1. The Parties shall execute all such further documents promptly and when required, and shall do or perform, or cause to be done or performed, all such acts as shall be reasonably necessary to give effect to this Termination Agreement.

8.2. The laws of the Province of British Columbia govern this Termination Agreement without giving effect to any choice or conflict of law provisions, principle or rule. All provisions of the International Sale of Goods Act (British Columbia) are specifically excluded from application to this Termination Agreement.

8.3. The Parties irrevocably submit to the exclusive jurisdiction of the Courts of the Province of British Columbia in respect of the enforcement hereof and resolution of any disputes hereunder.

8.4. This Termination Agreement shall inure to the benefit of and be binding upon each of the Parties and their respective Affiliates, partners, administrators, trustees, receivers, successors and permitted assigns.

8.5. This Termination Agreement supersedes all other agreements, documents, writings and verbal understandings among the parties relating to the subject matter hereof and expresses the entire agreement of the Parties with respect to the subject matter hereof. Any revisions, changes, or amendments hereto shall be in writing duly executed by the Parties.

8.6. This Termination Agreement may be executed in separate counterparts by facsimile, PDF or DocuSign or by original document and all the executed counterparts together shall constitute one agreement but no execution hereof shall be effective until all of the counterparts have been executed and delivered to each of the Parties.

[*Remainder of page intentionally left blank; Signature page follows*]

The Parties are signing this Termination Agreement on the date stated in the introductory clause.

CITY OF VANCOUVER

Per: s.15(1), s.22(1)

Name: Lon LaClaire
Title: General Manager of Engineering

Per: s.15(1), s.22(1)

Name: Frances J. Connell, K.C.
Title: Director of Legal Services

ZECO SYSTEMS CANADA INC.

Per: _____

Name:
Title:

ZECO HOLDINGS, INC.

Per: _____

Name:
Title:

ZECO SYSTEMS, INC.

Per: _____

Name:
Title:

The Parties are signing this Termination Agreement on the date stated in the introductory clause.

CITY OF VANCOUVER

Per: _____

Name:
Title:

Per: _____

Name:
Title:

Per: _____

Name:
Title:

ZECO SYSTEMS CANADA INC.

DocuSigned by:
Per: s.15(1), s.22(1)
5E612628EAC9429...

Name: Erich Stilling
Title: Director

ZECO HOLDINGS, INC.

DocuSigned by:
Per: s.15(1), s.22(1)
F7D21E7096AD4A5...

Name: Kuan Archer
Title: Chief Executive Officer

ZECO SYSTEMS, INC.

DocuSigned by:
Per: s.15(1), s.22(1)
F7D21E7096AD4A5...

Name: Kuan Archer
Title: Chief Executive Officer

Appendix A – Payment Breakdown

	Amounts owed to SRS	CoV Claims
Fleets	$293,924	$240,000
MURBS	$91,925	$189,000
Public Network	$80,837	$143,000
Total	**$466,685**	**$572,000**

Amounts owed to SRS as of 5.15.25	$466,685.32
PST reduction	15,762.42
Open invoices & PST reduction	$450,922.90
COV amounts claimed (less the credit owed for Sky overpayment of $56k)	516,000.00
Preliminary amount owed to Vancouver	65,077.10
Refund for prepaid licenses/unapplied payments	41,046.68
Net amount owed to Vancouver	**$106,123.78**

SUPPLY AGREEMENT

AMONG:

ZECO SYSTEMS (CANADA) INC.

ZECO HOLDINGS, INC.

ZECO SYSTEMS, INC.

AND:

CITY OF VANCOUVER

RELATING TO SUPPLY OF EV CHARGING EQUIPMENT AND SERVICES

RFP PS20180339

DATED JUNE 22nd, 2021

SUPPLY AGREEMENT

THIS AGREEMENT is made as of the 22nd day of June, 2021,

AMONG:

ZECO SYSTEMS (CANADA) INC., a corporation organized under the laws of Canada and having an office at 767 S. Alameda St., Suite 200, Los Angeles, California 90021

(hereinafter referred to as the "**Supplier**")

AND:

ZECO SYSTEMS, INC., a corporation organized under the laws of Delaware and having an office at 767 S. Alameda St., Suite 200, Los Angeles, California 90021

(hereinafter referred to as "**Zeco Systems**")

AND:

ZECO HOLDINGS, INC., a corporation organized under the laws of Delaware and having an office at 767 S. Alameda St., Suite 200, Los Angeles, California 90021

(hereinafter referred to as "**Zeco Holdings**" and together with Zeco Systems, each a "**Supplier Guarantor**" and collectively the "**Supplier Guarantors**")

AND:

CITY OF VANCOUVER, a municipal corporation continued under the *Vancouver Charter* (British Columbia) and having an office at 453 West 12th Avenue, Vancouver, British Columbia, V5Y 1V4

(hereinafter referred to as the "**City**")

WHEREAS the Supplier is in the business of selling the electric vehicle charging goods and services described in this Agreement;

AND WHEREAS the City wishes to procure such electric vehicle charging goods and services from the Supplier upon and subject to the terms and conditions hereinafter set forth,

AND WHEREAS the Supplier and Zeco Systems are the wholly-owned subsidiaries of Zeco Holdings, and the Supplier Guarantors have agreed to guarantee all of the obligations of Supplier under this Agreement,

NOW THEREFORE, in consideration of the premises and the covenants herein contained, the Parties and the Supplier Guarantors hereto agree as set forth herein.

TABLE OF CONTENTS

Page

ARTICLE 1
INTERPRETATION

1.1 Definitions

In this Agreement, each word or combination of words, whether or not capitalized, that is specifically defined will have the meaning given as defined. Any word or combination of words, whether or not capitalized, that is used in this Agreement and that is not specifically defined, where the context suggests a meaning similar to a meaning given in a defined term will have the same meaning as that defined term. In accordance with the foregoing:

(a) "**Agreement**" means this agreement, including the schedules hereto, and all amendments made hereto or thereto by written agreement between the Supplier and the City;

(b) "**Applicable Privacy Laws**" includes the *Freedom of Information and Protection of Privacy Act* (British Columbia) (FOIPPA); the *Personal Information Protection Act* (British Columbia) (PIPA) and the *Personal Information Protection and Electronic Documents Act* (Canada) (PIPEDA);

(c) "**Background IP**" has the meaning ascribed thereto in Section 14.4;

(d) "**Business Day**" means a day on which banks are open for business in Vancouver, British Columbia, except a Saturday, Sunday or statutory holiday;

(e) "**Change in Control**" means an occurrence whereby a person (or persons acting in concert) acquires control of the relevant entity;

(f) "**City Policies**" means any or all (as the context requires) of those procedures, standards and/or standard specifications, requirements, policies and the like listed in Schedule J (City Policies) or notified to the Supplier from time to time, as the same may be updated, modified, expanded, revised, supplemented and/or replaced from time to time by the City (as notified to the Supplier);

(g) "**City's Manager**" means a manager who at the relevant time carries such designation from the City under, or in accordance with, ARTICLE 5;

(h) "**Commissioning**" or "**Commissioned**" means, in reference to each Charging Unit (as such term is defined in Schedule H (Terms and Conditions Relating to O&M)) to which this term relates, (i) the electrical connection and energization of such Charging Unit by the electric utility, and (ii) the connection of such Charging Unit to Supplier's SKY™ Network such that the Charging Unit is ready for the City to commence operation;

(i) "**Competent Authority**" means:

(i) any multinational, federal, provincial, state, regional, municipal, local or other government or governmental body and any ministry, department, division, bureau, agent, agency, commission, board or authority of any government or governmental body, domestic or foreign;

(ii) any domestic, foreign or international judicial, quasi-judicial or administrative court, tribunal, commission, board, panel, arbitrator or arbitral body acting under the authority of any of the foregoing; or

(iii) any quasi-governmental or private body exercising any statutory, regulatory, expropriation or taxing authority under the authority of any of the foregoing;

(j) "**Confidential Information**" means all or any confidential information (however recorded or preserved) disclosed before, on or after the date of this Agreement by either Party or any of its Representatives to the other Party or its Representatives in connection with this Agreement, concerning:

(i) this Agreement; or

(ii) the affairs, operations, processes, know-how, suppliers, plans or intentions of the disclosing Party or of any member of the disclosing Party's Group, including, without limitation, any information which is not generally known to the public or which has been specifically identified as confidential or proprietary by the disclosing Party,

but does not include:

(iii) any information that is or becomes generally available to the public or to industry professionals (other than as a result of its disclosure by the receiving Party or its Representatives in breach of this Agreement);

(iv) any information that was available to the receiving Party on a non-confidential basis prior to disclosure by the disclosing Party;

(v) any information that was, is or becomes available to the receiving Party on a non-confidential basis from a person who, to the receiving Party's knowledge, is not bound by a confidentiality agreement or other duty of confidentiality with or to the disclosing Party or a member of the disclosing Party's Group or otherwise prohibited from disclosing the information to the receiving Party;

(vi) any information that was known to the receiving Party before the information was disclosed to it by the disclosing Party or its Representatives and was not subject to a confidentiality agreement or other duty of confidentiality (including any obligation under this Agreement) with or to the disclosing Party or a member of the disclosing Party's Group;

(vii) any information that the Parties agree in writing is not confidential or may be disclosed; and

(viii) any information unrelated to this Agreement that is developed by or for the receiving Party independently of and without reference to the information disclosed by the disclosing Party;

(k) "**Consent**" means an approval, clearance, registration, franchise, right, privilege, certification, quota, consent, permit, licence, qualification, filing, exemption, certificate or permission and any such other matter or authorization whatsoever, including any condition thereof, that is lawfully and necessarily required under any Law or from any Competent Authority in connection with the Supply or the Site;

(l) "**Contract Price**" means the amounts payable (subject to and in accordance with the terms of this Agreement) by the City to the Supplier in return for the proper performance by the Supplier of its obligations under this Agreement, as detailed in Schedule B (Prices for Supply), Schedule G (Terms and Conditions relating to Software) and Schedule H (Terms and Conditions relating to O&M);

(m) "**Defect**" means any part of the Supply (or omission therefrom) which is defective, deficient or incomplete or does not otherwise comply with the requirements of this Agreement which is identified prior to written acceptance or deemed acceptance by the City pursuant to Section 3.12(b);

(n) "**Delivery**" means the completion of delivery of goods or products ordered in a particular purchase order, in accordance therewith and herewith;

(o) "**Delivery Date**" has the meaning ascribed to such term in Section 3.6(a);

(p) "**Delivery Location**" has the meaning ascribed to such term in Section 3.6(a);

(q) "**Documentation**" means calculations, computer programs and other software, drawings, designs, plans, manuals, records, reports, documents, papers, photos, typographical arrangements, models, contract documents, deliverables, agreements, tender/enquiry documents, and all other materials in whatever form, including but not limited to tangible copies and electronic forms, supplied either by or on behalf of the Supplier or generated collaboratively by the Parties in the course of the provision of the Supply under this Agreement; provided that Documentation does not include any of the foregoing that relates the Background IP of the Supplier;

(r) "**Effective Date**" has the meaning ascribed to such term in Section 2.1;

(s) "**Encumbrance**" means any mortgage, charge, pledge, hypothecation, security interest, assignment, lien or claim of lien (statutory or otherwise), easement, deemed or statutory trust, restrictive covenant, adverse claim, exception, reservation, right of occupation, any matter capable of registration against title, right of pre-emption, privilege or other encumbrance or third party right of any nature or any other arrangement or condition that, in substance, secures payment or performance of an obligation;

(t) "**Environmental Law**" means any Law which imposes any obligations relating to:

(i) the protection, management, conservation or restoration of the natural environment;

(ii) reporting, licensing, permitting, investigating, remediating and cleaning up in connection with any presence or Release, or the threat of the same, of Hazardous Substances; and

(iii) the manufacture, processing, distribution, use, treatment, storage, disposal, transport, handling and the like of Hazardous Substances, including those pertaining to occupational health and safety;

(u) "**FOIPPA**" means the Freedom of Information and Protection of Privacy Act (British Columbia) as it may be amended or superseded from time to time;

(v) "**Force Majeure**" means, exhaustively, any:

(i) war, hostilities (whether war is declared or not), invasion, act of foreign enemies;

(ii) rebellion, terrorism (or threat of terrorism), revolution, insurrection, military or usurped power or civil war;

(iii) riot, civil commotion or disorder, strike or lockout by persons other than the Supplier's personnel and other employees, Subcontractors or any other person for whom the Supplier is responsible;

(iv) natural catastrophe such as an earthquake, forest fire, landslide or flood; or

(v) change in Law or action by a Competent Authority, which makes it illegal or impossible for either Party or the Supplier Guarantors to perform their respective obligations under this Agreement;

(w) "**Good Industry Practice**" means, in relation to the Supply or the performance of any other obligation under this Agreement, the practices, and the application of the skill, care, diligence, prudence and foresight, which would reasonably and ordinarily be expected from a skilled and experienced international contractor carrying out or procuring equivalent services of similar type, scope and value, in the same or similar location and in similar circumstances to those pertaining to the Supplier;

(x) "**Group**" means:

(i) in respect of the Supplier, the group constituted from time to time by:

(A) the Supplier; and

(B) all persons that directly or indirectly control or are controlled by the Supplier; and

(ii) in respect of the City, the group constituted from time to time by:

(A) the City; and

(B) all bodies corporate directly or indirectly controlled by the City.

(y) "**Hazardous Substance**" means any substance or material that is prohibited, controlled or regulated by any Competent Authority pursuant to any Environmental Law including pollutants, contaminants, dangerous goods or substances, toxic or hazardous substances or materials, wastes (including solid non-hazardous wastes and subject wastes), petroleum and its derivatives and by-products and other hydrocarbons, all as defined in or pursuant to any Environmental Law;

(z) "**Intellectual Property Rights**" means any and all current and future proprietary rights provided under patent law, copyright law, design patent or industrial design law, or any other applicable statutory provision or common law principle, including trade secret law, that may provide a right in ideas, formulae, algorithms, concepts, inventions, know-how, computer software, database or design, or the expression or use thereof, whether registered or unregistered, together with any right to apply for or register any of the foregoing;

(aa) "**Key Project Personnel**" means the persons named in Schedule K (Key Project Personnel) and any replacement(s) approved by the City in accordance with ARTICLE 7;

(bb) "**Laws**" means all laws, statutes, codes, ordinances, decrees, rules, regulations, by-laws, judicial or arbitral or administrative or ministerial or departmental or regulatory judgments, orders, decisions, rulings, determinations or awards of any Competent Authority and any legal requirements or bases of liability under the common law or civil law, including all such Laws relating to Taxes, the environment, human health or safety,

pollution and other environmental degradation, and hazardous materials , which affect or are otherwise applicable to the Supply, the Supplier, the Site or any other lands affected by the Supply;

(cc) "**Living Wage**" means the hourly wage established by the Living Wage Certifier from time to time during the Term, which, as of the Effective Date, is $20.62 per hour, which includes: (i) direct wages; and (ii) the value of any non-mandatory benefits such as paid sick leave, employer-paid Medical Services Plan premiums and extended health benefits;

(dd) "**Living Wage Certifier**" means the Living Wage for Families Campaign, any successor entity, or, in the event the Living Wage for Families Campaign ceases to carry on operations, such other living wage certification entity designated by the City to the Supplier in writing;

(ee) "**Living Wage Employee**" means any and all employees of the Supplier and Subcontractors of the Supplier that perform any part of the Supply on a property owned by or leased to the City, including all streets, sidewalks and other public rights of way, for at least one consecutive hour, but excluding Students, volunteers and employees of Social Enterprises;

(ff) "**Mechanical Completion**" means, in reference to each Charging Unit (as such term is defined in Schedule H (Terms and Conditions Relating to O&M)) to which this term relates, (i) the date when Supplier or its Subcontractor notifies the City in writing that construction of such Charging Unit at a Site is substantially complete, (ii) the applicable Competent Authority and electric utility have performed inspections and given all necessary approvals, and the Charging Unit is only waiting on the electric utility to make the electrical connection and energize it;

(gg) "**OHS Requirements**" means all Laws applicable to the Supply and related to occupational health or safety, and all of the City Policies that relate to occupational health or safety, and includes without limitation the WCA;

(hh) "**Parties**" means the City and the Supplier and "**Party**" means one of them or either of them, as the context requires;

(ii) "**Permitted Purpose**" has the meaning ascribed thereto in Section 15.3;

(jj) "**Personal Information**" or similar terms used in this Agreement, whether or not capitalized, means "personal information" as such term is defined in Applicable Privacy Laws;

(kk) "**Proposal**" means the Supplier's proposal dated February 26, 2019, submitted by the Supplier to the City in response to the RFP;

(ll) "**Release**" means any release or discharge of any Hazardous Substance including any discharge, spray, injection, inoculation, abandonment, deposit, spillage, leakage, seepage, pouring, emission, emptying, throwing, dumping, placing, exhausting, escape, leach, migration, dispersal, dispensing or disposal;

(mm) "**Representative**" means a Group member of a Party, or an official, officer, employee, agent, subcontractor or other representative of a Party or any member of its Group, or any other person for whom the Party is responsible;

(nn) "**RFP**" means the City's Request for Proposal number PS20180339;

(oo) "**Safety Incident**" means:

(i) a failure by the Supplier or any Subcontractor to comply with any OHS Requirements; or

(ii) any hazard, incident, accident or any other circumstances, whether or not caused by the Supplier or a Subcontractor, deemed unsafe to the public as determined by the City acting reasonably;

(pp) "**Sales Tax**" has the meaning ascribed to such term in Section 16.1;

(qq) "**Site**" means a City building or other City worksite at which any part of the Supply shall be performed;

(rr) "**Social Enterprise**" means a business that: (i) is owned by a non-profit organization or community services co-operative; (ii) is directly involved in the production and/or selling of goods and services for the combined purpose of generating income and achieving social, cultural, and/or environmental aims; and (iii) has a defined social and/or environmental mandate.;

(ss) "**Student**" means an individual who is enrolled in a school, college, university or other educational institution and is employed by the Supplier or a Subcontractor, as the case may be, to obtain practical workplace experience as a requirement of or credit for their education;

(tt) "**Subcontractor**" means any person named in a schedule to this Agreement as a subcontractor, or any other person appointed by the Supplier, in accordance with this Agreement, to perform any part of the Supply;

(uu) "**Supplier's Manager**" means a manager who at the relevant time carries such designation from the Supplier under, or in accordance with, ARTICLE 5;

(vv) "**Supply**" means the provision of the goods, services and works described in Schedule A (Scope of Goods and Services) (or, as the context requires, the particular such goods, services or works provided or to be provided by the Supplier to the City at a particular time or times and in the particular combinations and quantities directed by the City in accordance herewith), and any other goods or services to be provided by the Supplier pursuant to this Agreement;

(ww) "**Taxes**" means all taxes, duties, imposts, levies, assessments, tariffs and other charges imposed, assessed or collected by a Competent Authority, including:

(i) any gross income, net income, gross receipts, business, royalty, capital, capital gains, goods and services, harmonized sales, value added, severance, stamp, franchise, occupation, premium, capital stock, sales and use, real property, land transfer, personal property, ad valorem, transfer, licence, import, customs, profits, windfall profits, environmental, carbon, emissions, pollution, payroll, employment, employer health, pension plan, anti-dumping, countervailing, or excise tax, duty, import, levy, assessment, tariff or other charge;

(ii) all withholdings on amounts paid to or by the relevant person;

(iii) all statutory remittances, employment insurance premiums and social security or pension plan contributions or premiums and Canada pension plan contributions;

(iv) any fine, penalty, interest or addition to tax;

(v) any tax imposed, assessed, or collected or payable pursuant to any tax-sharing agreement or any other contract relating to the sharing or payment of any such tax, levy, assessment, tariff, duty, deficiency or fee; and

(vi) any liability for any of the foregoing as a transferee, successor, guarantor, or by contract or by operation of law;

(xx) "**Time(s) for Completion**" means the time(s) stated in Schedule C (Deployment Plan) by which the Supply or any particular Supply or part thereof must be completed, as such time(s) may be adjusted (including in relation to a particular instance of Supply), strictly in accordance with this Agreement;

(yy) "**Variation**" has the meaning ascribed to such term in Section 3.11(a); and

(zz) "**WCA**" means the *Workers Compensation Act* (British Columbia) and the regulations thereunder.

1.2 Headings

This division of this Agreement into articles and sections and the insertion of headings are for convenience of reference only and do not affect the construction or interpretation of this Agreement. The terms "hereof", "hereunder" and similar expressions refer to this Agreement, including its schedules, and not to any particular article, section or other portion hereof. Unless something in the subject matter or context is inconsistent therewith, references herein to articles, sections and schedules are to articles, sections and schedules of this Agreement.

1.3 Extended Meanings

In this Agreement:

(a) words importing the singular include the plural and vice versa, words importing a gender include all genders and words importing persons include individuals, partnerships, associations, trusts, unincorporated organizations and corporations, except where the context requires otherwise;

(b) any provision calling for "agreement" requires the relevant agreement to be recorded in writing and signed by both Parties;

(c) the words "include", "includes", "including" and "included" shall be construed without implying limitation by the words which follow those words and without prejudice to the generality of the provisions to which such words relate, unless inconsistent with the context, and the rule of interpretation known as ejusdem generis shall not apply;

(d) each reference to a specific statute, regulation, law or any subordinate instrument or statutory or regulatory provision shall be construed as including any legal or regulatory provision which subsequently amends or replaces the same, and shall include any and all subordinate instruments, orders, rules, regulations and bylaws made thereunder or guidelines issued in respect thereof;

(e) each reference to a writing means a writing that is hand-written, type-written, printed or electronically made, and which results in a permanent un-editable record; and

(f) "control" when used to describe a relationship between one person and any other person, has the following meanings:

(i) a person controls a body corporate if securities of the body corporate to which are attached more than 50% of the votes that may be cast to elect directors of the body corporate are beneficially owned by the person and the votes attached to those securities are sufficient, if exercised, to elect a majority of the directors of the body corporate;

(ii) a person controls an unincorporated entity, other than a limited partnership, if more than 50% of the ownership interests, however designated, into which the entity is divided are beneficially owned by that person and the person is able to direct the business and affairs of the entity;

(iii) the general partner of a limited partnership controls the limited partnership; and

(iv) a person who controls an entity is deemed to control any entity that is controlled, or deemed to be controlled, by the entity.

1.4 Schedules

The following are the schedules hereto, each of which is deemed to be part hereof:

1)	Schedule A	Scope of Goods and Services • Appendix 1 – Format of Report required by 8.1(a) and 8.1(b)
2)	Schedule B	Prices for Supply
3)	Schedule C	Deployment Plan
4)	Schedule D	PCI Requirements • Appendix 1 – Cardholder Data Services and Cashflow Diagram • Appendix 2 - PCI DSS Responsibility Matrix • Appendix 3 – Letter Template
5)	Schedule E	Appendix 1 - Additional Privacy and Data Security Requirements • Appendix 2 – Privacy Requirements
6)	Schedule F	Technology Requirements • Appendix 1 – Technology - CAIQ
7)	Schedule G	Terms and Conditions Relating to Software
8)	Schedule H	Terms and Conditions Relating to O&M
9)	Schedule I	Roaming and Interoperability
10)	Schedule J	City Policies
11)	Schedule K	Key Project Personnel
12)	Schedule L	Appendix 1 - Insurance Requirements • Appendix 2 – Copy of Valid Certificate provided by Supplier on date of Agreement
13)	Schedule M	RFP
14)	Schedule N	Proposal

In the event of any conflict or inconsistency between any of the terms of the body of this Agreement and any terms of a schedule, the terms of the body of the Agreement will govern and prevail. In the event of any conflict or inconsistency between any of the schedules, the schedules set out in the above order will govern and prevail.

ARTICLE 2
EFFECTIVENESS

2.1 Effective Date

This Agreement shall come into full force and effect on the date hereof (the "**Effective Date**").

2.2 Term

(a) Unless earlier terminated pursuant to ARTICLE 12 and subject to the below Section 2.2(b), this Agreement shall terminate on the 5th anniversary of the Effective Date or on such later date as the Parties may agree in writing.

(b) Subject to termination pursuant to ARTICLE 12, but notwithstanding Section 2.2(a), the term of this Agreement may be extended for up to four one-year extensions following the 5th anniversary of the Effective Date for a maximum term of up to nine (9) years from the Effective Date, at the option of the City, upon written notice from the City to the Supplier.

(c) For certainty:

(i) if the City elects to extend this Agreement following the initial 5 year term, the City may, but is not required to, also extend any or all of the services described in Schedule G (Terms and Conditions relating to Software), or in Schedule H (Terms and Conditions relating to O&M); and

(ii) at any time during the term of this Agreement, the City may, but is not required to, change the applicable plan in respect of operation and maintenance services to be provided by the Supplier, subject to the applicable terms and conditions set forth in Schedule H (Terms and Conditions relating to O&M).

(d) Notwithstanding the foregoing, if the City and the Supplier continue to deal with each other in respect of the subject matter of this Agreement following the expiry of this Agreement, without any additional or other written agreement in respect thereof, this Agreement shall be deemed to have been renewed on a month-to-month basis on the same terms and conditions as before the expiry of the Agreement and it may be cancelled without cause by either Party on thirty (30) days' prior written notice to the other.

ARTICLE 3
SUPPLY; GENERAL TERMS

3.1 Supply

(a) During the term of effectiveness of this Agreement, the Supplier shall provide the Supply to the City at the Sites directed by the City, at the times and in the quantities directed by the City, and otherwise in accordance with the directions of the City and in conformity with this Agreement.

(b) Notwithstanding any other provision hereof, any goods, services or works described in Schedule A (Scope of Goods and Services) shall be provided to the City only upon receipt by the Supplier of a purchase order from the City or another instruction given by the City pursuant to Section 5.1 relating to such Supply.

(c) The Supplier shall maintain at all times sufficient business capacity and inventories of the supplies necessary for the provision of the Supply, to meet the business plans and requirements of the City.

(d) In connection with the Supply, the Supplier shall provide to the City, for the agreed compensation, all services, conveniences, materials or features that are reasonably inferable from the descriptions of the Supply herein.

3.2 Application to Prior Acts

Insofar as the Supplier has commenced any part of the Supply prior to the Effective Date, such services shall, as of the Effective Date, be deemed to be performed under and subject to the terms of this Agreement, unless otherwise expressly agreed between the Supplier and the City.

3.3 Sufficiency and Competence of Personnel

(a) The Supplier shall have and maintain at all times and in accordance with all applicable Laws, sufficient numbers of fit, skilled, qualified and experienced personnel to carry out the provision of the Supply within the times and in the manner required by the City.

(b) The Supplier warrants that it has (and its Subcontractors, if any, have) the experience, competence, certifications, qualifications and capacity necessary for the Supply.

3.4 Standards and Requirements

The Supplier shall (and shall procure that its Subcontractors) provide the Supply and perform all other obligations under this Agreement in an expeditious manner and at all times in materially in accordance with:

(a) all applicable Laws and Consents;

(b) the specific requirements of Schedule A (Scope of Goods and Services) and Schedule C (Deployment Schedule), and the instructions of the City;

(c) the City Policies; and

(d) where no higher standard is expressly required of the Supplier under this Agreement, Good Industry Practice,

and the Supplier shall materially comply with the standards and requirements in Sections 3.4(a)to 3.4(d) in the order of priority in which such standards or requirements are listed (with Section 3.4(a) being of highest priority).

3.5 Consents

The Supplier shall, at the Supplier's sole expense, obtain, maintain and comply with all Consents required by Law to enable it to perform its obligations under this Agreement, except to the extent otherwise expressly stated in the schedules hereto.

3.6 Goods Orders

(a) Notwithstanding any other provision hereof, the City shall not order any goods or materials hereunder except pursuant to a written purchase order, which must:

(i) be given in writing;

(ii) refer to this Agreement;

(iii) specify the goods and materials ordered; and

(iv) specify a date pre-agreed upon by the Supplier and the City by which the goods and materials ordered pursuant to the purchase order are to be delivered (the "**Delivery Date**"), and the location or address to which they are to be delivered (the "**Delivery Location**"), provided that the Delivery Location for each order must be a Site.

3.7 Delivery Requirements

(a) The Supplier shall, if applicable, pack, transport and supply all goods and materials forming part of the Supply in accordance with all:

(i) manufacturer recommendations and requirements;

(ii) generally accepted industry standards and practices; and

(iii) applicable Laws.

(b) The Supplier shall ensure that all goods and materials are properly packed and secured in such manner as to enable them to reach their destination in good condition.

(c) The Supplier shall deliver all goods or materials ordered by the City hereunder to the applicable Delivery Location by the applicable Delivery Date.

(d) Delivery of the goods or materials specified in a purchase order shall be complete only upon the completion of their unloading at the Delivery Location.

(e) Each shipment of goods or materials shall be accompanied by a delivery document from the Supplier showing the purchase order number, the date of the purchase order, the type and quantity of goods or materials included in the shipment, and, in the case of an order being delivered by instalments, the outstanding balance of goods or materials remaining to be delivered.

(f) If the Supplier requires the City to return any shipping containers, or other packaging or shipping materials, to the Supplier, that fact must be clearly stated on the delivery document accompanying the relevant goods or materials, and any such return shall be at the Supplier's expense.

(g) In respect of any goods or materials that originate outside Canada, the Supplier shall be responsible for all customs and import Taxes, costs, expenses, administrative duties and formalities.

3.8 Rejection of Defective goods or materials

(a) The Supplier shall test all goods and materials prior to their delivery to the City to confirm they function correctly, and as intended, except for goods and materials that are delivered directly to the City and are not configured by the Supplier.

(b) If any goods or materials delivered to the City do not comply with Schedule A (Scope of Goods and Services) or the Proposal, or are otherwise not in conformity with the terms of this Agreement, then, without limiting any other right or remedy that the City may have, the City may at any time reject those goods or materials and:

(i) require the Supplier to remove the rejected goods or materials from any facility or work site of the City at the Supplier's risk and expense within ten Business Days of being requested to do so;

(ii) require the Supplier to repair or replace the rejected goods or materials at the Supplier's risk and expense within 20 Business Days of being requested to do so; and

(iii) claim damages for any costs, expenses or losses resulting from the Supplier's delivery of goods or materials that are not in conformity with the terms of this Agreement.

(c) The City's rights and remedies under this Section 3.8 are in addition to the rights and remedies available to it under other sections of this Agreement and applicable Laws.

(d) The terms of this Agreement shall apply to any repaired or replacement goods or materials supplied by the Supplier pursuant to Sections 3.8 or 3.9.

3.9 Warranties

(a) The Supplier warrants that the Supply shall be performed in accordance with this Agreement and to the best practice standards of diligence, skill, care and efficiency expected of a competent contractor performing work of a similar nature to the Supply.

(b) All goods or materials provided under the Agreement as part of the Supply shall be new and shall have the warranties applicable to the Supply as set forth in the Schedules attached hereto.

(c) All goods, works and materials provided under the Agreement as part of the Supply shall be non-defective and fit for their intended purposes and shall function safely in all respects.

(d) The Supplier shall deliver to the City all such documentation as the City may require to evidence any warranty required by this Section 3.9 or to evidence the Supplier's compliance with this Section 3.9, and the Supplier shall assign all warranties, and do all other things reasonably necessary, to ensure that the City receives the full benefit of each warranty or other covenant set forth in this Section 3.9.

(e) EXCEPT AS EXPRESSLY DESCRIBED IN THIS AGREEMENT, THE SUPPLY PROVIDED BY SUPPLIER OR ITS SUBCONTRACTORS PURSUANT TO THE TERMS OF THIS AGREEMENT ARE PROVIDED ON AN "AS IS" BASIS. EXCEPT FOR THE WARRANTIES EXPRESSLY SET FORTH IN THIS AGREEMENT, SUPPLIER DISCLAIMS ANY AND ALL WARRANTIES, WHETHER WRITTEN, EXPRESS OR IMPLIED, WITH RESPECT TO THE SUPPLY, INCLUDING ANY WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, AND ALL WARRANTIES ARISING OUT OF USAGE OF TRADE, COURSE OF DEALING OR COURSE OF PERFORMANCE.

(f) SUPPLIER DISCLAIMS ALL WARRANTIES WITH RESPECT TO ANY PORTION OF THE SUPPLY PROVIDED OR PERFORMED BY A MANUFACTURER OF THE SUPPLY PURSUANT TO ANY WARRANTY PROVIDED BY SUCH MANUFACTURER OR ANY EXTENDED WARRANTY OF SUCH MANUFACTURER PURCHASED BY THE CITY THROUGH SUPPLIER.

3.10 Relationship Between the Parties

(a) The Supplier in its provision of the Supply and its performance of its obligations under this Agreement shall at all times act as an independent contractor on its own account

and shall have no authority to act as the City's agent unless expressly empowered to do so by the City. This Agreement shall not be deemed to create any relationship of partnership, agency, joint enterprise or other like relationship between the Parties, and the Supplier shall be solely responsible for all employment-related obligations in connection with its employees, its other Representatives and its Subcontractors and their employees.

(b) This Agreement is not an exclusive supply arrangement and the City is not bound to treat the Supplier as its exclusive supplier of any goods or services.

3.11 Variations Requested by the City

(a) Any instruction given by the City which constitutes or gives rise to a variation from the scope of the Supply expressed in Schedule A (Scope of Goods and Services) or a time expressed in Schedule C (Deployment Plan), shall constitute a "Variation" and shall be governed by and subject to this Section 3.11.

(b) During the term of this Agreement, the City may at any time effect a Variation by notice in writing to the Supplier, and the Supplier shall not be entitled to refuse to implement any Variation unless the carrying out of such Variation would contravene any Law (in which case the Supplier shall promptly give notice to the City).

(c) If the Supplier is of the opinion that a Variation justifies an increase to the Contract Price or a change to any of the Time(s) for Completion, the Supplier must, as a condition to being entitled to any such increase to the Contract Price or change to the Time(s) for Completion, no later than 10 Business Days after Supplier receives written notice of the Variation, submit a claim to the City which sets out the Supplier's assessment of the impact the Variation should have on the Contract Price due for such Supply and on the Time(s) for Completion for such Supply, and thereafter:

(i) the City shall consider that claim as soon as possible and may request the Supplier to supply such further evidence as is reasonably required to confirm the details of such claim (and, as soon as practicable after such further evidence is available to it, the Supplier shall provide it to the City); and

(ii) within ten Business Days after the receipt of all the information requested by the City, the Supplier and the City shall meet in order to agree any variations to the Contract Price for such Supply or the Time(s) for Completion for such Supply, which such agreement must be evidenced in writing.

(d) If no agreement is reached under 3.11(c)(ii) within 20 Business Days of the Parties' first meeting (or such other period as the Parties may agree), the Parties may then refer the matter for arbitration in accordance with ARTICLE 17.

(e) Notwithstanding the foregoing, the City shall be entitled to replace, revise, expand or modify the City Policies at any time upon notice to the Supplier, and no such change shall be considered to be a Variation unless any such change increases the Contract Price or changes the Time(s) for Completion.

3.12 Tests; Defects and Acceptance

(a) When, in the Supplier's judgement, any part of the Supply is complete in accordance herewith, the Supplier shall give written notice to that effect to the City. Thereafter but prior to written acceptance or deemed acceptance by the City pursuant to Section 3.12(b), the City shall reasonably promptly perform such practical tests of the Supply as

the City reasonably deems necessary, and the Supplier shall assist the City with all such tests, if and to the extent so requested by the City.

(b) If a Defect appears in the Supply or the testing described in the foregoing Section 3.12(a) reveals, in the reasonable judgement of the City, any Defects in the Supply, the City shall notify the Supplier accordingly. The City shall, as soon as reasonably practicable after receipt of Supplier's notice pursuant to Section 3.12(a), provide written notice to Supplier of its acceptance of the Supply; provided that City's failure to provide any such notice within fifteen (15) Business Days of receipt of written notice from Supplier shall result in such portion of the Supply being deemed accepted by the City.

(c) The Supplier shall remedy at its own cost and risk Defects in the Supply that the Supplier discovers or that are notified by the City, as soon as reasonably practicable following discovery or notification of such Defects, as the case may be.

(d) If the Supplier fails to remedy any Defect in the Supply within a reasonable time, a date may be fixed by the City on or by which the Defect is to be remedied. The Supplier shall be given reasonable notice of this date.

(e) If the Supplier fails, without reasonable excuse, to remedy any Defect in the Supply by this notified date, the City may (at its option) elect to carry out the work itself or by others and shall be entitled to recover from the Supplier all direct, proper and reasonable costs of so doing (as a debt due on demand). The City's exercise of its election under this Section 3.12(e) shall in no event absolve the Supplier of its responsibility for remediation of other Defects or otherwise constitute a waiver by the City of its rights and remedies in relation to other Defects, nor shall it preclude or restrict the further exercise of such rights or remedies.

3.13 Title and Risk

(a) The Supplier warrants that title in each good, work or improvement supplied by the Supplier hereunder, when it passes to the City hereunder, shall be free and clear of Encumbrances.

(b) Title to any good, work or improvement supplied by the Supplier hereunder shall pass to the City upon the earlier of:

(i) payment therefor by the City;

(ii) its installation and commissioning at any part of a Site;

(iii) its incorporation into a good or work supplied by the Supplier; or

(iv) the Delivery of a good to a Delivery Location owned or operated, and as requested, by the City,

all in accordance with the terms of this Agreement.

(c) The Supplier shall deliver to the City any documentation, including a bill of sale, which the City may reasonably require to evidence the transfer of title in and to goods to the City, free and clear of all Encumbrances.

(d) The Supplier must not enter any contract that reserves ownership of goods or materials supplied by the Supplier hereunder in favour of any third party and, at the request of

the City, the Supplier must provide evidence that no such contract has been entered into.

(e) Notwithstanding that title passes to the City as provided in Section 3.13(b), Supplier is responsible for the care of, and bears all of the risk of loss or damage to, each good, work or improvements supplied hereunder and each material used in connection with the Supply, until:

(i) in respect of all physical goods that are supplied, such time as such goods are turned over to the City and Supplier or its Subcontractors no longer have custody or control of such goods; or

(ii) in respect of any component of the Supply to which the terms Mechanical Completion or Commissioning apply, such time that such component of the Supply is Commissioned.

Notwithstanding the above, Supplier is not responsible for any loss or damage that is caused by the City or its Subcontractors unless Supplier contributed to such loss or damage in which case responsibility will be borne by the Parties in proportion to the loss or damage caused by each Party.

3.14 Living Wage

(a) Subject to Section 3.14(b), it is a condition of this Agreement that, for the duration of the Term the Supplier pays all Living Wage Employees not less than the Living Wage.

(b) Notwithstanding Section 3.14(a), the Supplier has up to 6 months from the date on which any increase in the Living Wage is published by the Living Wage Certifier to increase wages for all Living Wage Employees such that all Living Wage Employees continue to be paid not less than the Living Wage.

(c) The Supplier shall ensure that the requirements of Section 3.14(a) apply to all Subcontractors.

(d) A breach by the Supplier of its obligations pursuant to Sections 3.14(a) and (c) shall constitute a material breach by the Supplier of this Agreement that shall entitle the City to terminate this Agreement in accordance with Section 12.2(b).

(e) The Supplier shall prepare and submit to the City in a format reasonably acceptable to the City before January 31 of each calendar year of the term or, for each partial calendar year of the term, within 30 days of the expiry of the term a living wage report setting out:

(i) the number of Living Wage Employees of the Supplier and each Subcontractor who were paid a Living Wage pursuant to this Section 3.14 during the previous calendar year or portion thereof that would not have received a Living Wage for substantially similar work but for the obligations of the Supplier pursuant to this Section 3.14; and

(ii) the total incremental costs incurred by the Supplier, including any amounts paid to Subcontractors, in order to fulfill its obligations pursuant to this Section 3.14 to pay a Living Wage to the Living Wage Employees described in Section 3.14(e)(i).

ARTICLE 4
INTENTIONALLY DELETED

ARTICLE 5
CONTRACT MANAGERS

5.1 City's Managers

(a) The City hereby designates each of **Jason Bethell**, Business Support Manager (Streets) and **Duminda Epa**, Traffic and Electrical Operations and Design Branch Manager as a "City's Manager." Each City's Manager, including any additional City's Managers designated by the City in accordance herewith, has, for so long as he or she remains a City's Manager, full authority to act on behalf of the City in relation to all matters arising under this Agreement.

(b) Any instruction from the City to the Supplier pursuant to this Agreement shall be issued through an executive officer of the City or through a City's Manager and shall be effective if in writing or confirmed in writing within seven days of oral instruction. Failure to comply with this Section 5.1 shall render any purported City's instruction invalid, unless it is later ratified by the City. However, this restriction does not apply to any instruction issued in an emergency situation or which relates to a threat or potential threat to the life, health or safety of any individual.

(c) Notwithstanding the foregoing, each City's Manager may, in writing, delegate his or her authority hereunder to others.

5.2 Supplier's Managers

(a) The Supplier hereby designates each of **JT Steenkamp** and **John Murnin** as a "Supplier's Manager." Each Supplier's Manager, including any additional Supplier's Managers designated by the Supplier in accordance herewith, has, for so long as he or she remains a Supplier's Manager, full authority to act on behalf of the Supplier in relation to all matters arising under this Agreement, and any instruction given by the City to either of them shall be deemed to be valid and effective.

(b) Each Supplier's manager may, in writing, delegate his or her authority hereunder to others, upon the written agreement of the City.

5.3 Designation of New Managers

The City may designate new City's Managers, or remove that designation from any individual, and the Supplier may designate new Supplier's Managers, or remove that designation from any individual, from time to time, each at its own discretion, through notice to the other Party. In the case of the Supplier, any such designation or removal must be in writing to the City.

ARTICLE 6
SUPPLIERS' WARRANTIES AND COVENANTS

6.1 General Representations and Warranties

The Supplier represents and warrants that:

(a) the Supplier has the full right, power, and authority to enter into, and to perform all of its obligations under, this Agreement;

(b) the Supplier is a corporation duly organized, validly existing and in good standing under the laws of Canada and is lawfully authorized to do business in the Province of British Columbia;

(c) the Supplier will maintain its good standing and legal authority to do business in the Province of British Columbia for the duration of this Agreement without lapse or interruption;

(d) the Supplier is not a party to or bound by any agreement (written or oral), indenture, instrument, licence, permit or understanding or other obligation or restriction under the terms of which the execution, delivery or performance of this Agreement does or shall constitute or result in a violation or breach;

(e) all of the issued and outstanding shares of stock in the equity of the Supplier is registered to, and beneficially owned by, Zeco Holdings;

(f) it is a party to, and supplier under, other similar contracts for the supply, installation, operation or maintenance of EV charging goods and services to, for or behalf of, customers located in Canada;

(g) the Supplier is GST registered in Canada and will remain GST registered and in good standing for the duration of this Agreement without lapse or interruption;

(h) the Supplier has a valid City of Vancouver business license that applies to all of the Supply;

(i) all statements made by the Supplier in its Proposal were true and accurate when made;

(j) the Supplier is fully experienced in the design and management of projects or works of a similar scope, purpose, complexity, size and technical sophistication as the Supply;

(k) the Supplier possesses a level of skill and expertise commensurate with Good Industry Practice, which it shall utilize in the performance of its obligations under this Agreement;

(l) the Supplier understands that the City is relying upon the skill, judgment and expertise of the Supplier and its Subcontractors (if any) in the carrying out of the Supply and the co-ordination and planning thereof; and

(m) the Supplier's and any Subcontractors' employees are accredited to carry out the relevant portions of the Supply to the extent required by applicable Laws and all of them are appropriately skilled, competent and experienced and possess relevant qualifications having regard to the nature and extent of the Supply and the Sites;

Zeco Systems represents and warrants that:

(n) it has the full right, power, and authority to enter into, and to perform all of its obligations under, this Agreement;

(o) it is a corporation duly organized, validly existing and in good standing under the laws of the State of Delaware;

(p) it will maintain its good standing in the State of Delaware for the duration of this Agreement without lapse or interruption;

(q) it is not a party to or bound by any agreement (written or oral), indenture, instrument, licence, permit or understanding or other obligation or restriction under the terms of which the execution, delivery or performance of this Agreement does or shall constitute or result in a violation or breach;

(r) all of its issued and outstanding shares of stock are registered to, and beneficially owned by, Zeco Holdings; and

(s) it is a party to, and supplier under, other similar contracts for the supply, installation, operation or maintenance of EV charging goods and services to, for or behalf of, customers located in the United States.

Zeco Holdings represents and warrants that:

(t) it has the full right, power, and authority to enter into, and to perform all of its obligations under, this Agreement;

(u) it is a corporation duly organized, validly existing and in good standing under the laws of the State of Delaware;

(v) it will maintain its good standing in the State of Delaware for the duration of this Agreement without lapse or interruption;

(w) it is not a party to or bound by any agreement (written or oral), indenture, instrument, licence, permit or understanding or other obligation or restriction under the terms of which the execution, delivery or performance of this Agreement does or shall constitute or result in a violation or breach; and

(x) it is the registered and beneficial owner all of the issued and outstanding shares of stock in the equity of the Supplier and Zeco Systems.

6.2 General Health and Safety-Related Acknowledgements and Covenants

The Supplier shall:

(a) in the provision of the Supply, comply at all times with the OHS Requirements and take all reasonably necessary steps to ensure similar compliance from its Representatives and its Subcontractors, if any;

(b) if the Supply involves any type of manual labour, prior to their attendance at any Site, deliver to each of its Representatives and each of its Subcontractors, if any, and to their employees, if applicable, copies of the OHS Requirements relevant to the Site;

(c) at all times take all reasonable precautions to maintain the health and safety of workers;

(d) be at all times registered and in good standing with the relevant workers' compensation insurance Competent Authorities, and provide to the City copies of any notices, correspondence or directions issued by any government or Competent Authority relating to workplace-related employment, human rights, labour, immigration policy, health, safety or environmental matters within 24 hours of the Supplier's receipt of such notice, correspondence or direction;

(e) appoint a qualified health and safety coordinator to ensure coordination of health and safety activities in the provision of the Supply;

(f) report (with full details) any accident, injury, illness or other incident relating to workplace health and safety or the environment regarding the Supply to the City as soon as reasonably practicable, investigate the accident, injury, illness or other incident reasonably thoroughly (and in any event in accordance with any applicable OHS Requirements) and promptly report to the City the results of each such investigation;

(g) maintain such records and make such reports concerning health, safety and welfare of persons, and damage to property, or the natural, physical or biological environment, as the City may reasonably require; and

(h) to the extent a "prime contractor", as defined in the WCA, is not already designated by the City for any portion of a Site, be and act as the prime contractor, and the Supplier assumes and is wholly responsible for the health and safety of all persons at such locations on the basis described in the WCA.

6.3 Covenants Regarding Violations of Health and Safety Requirements

Without prejudice to any remedies available to the City hereunder, if any Subcontractor or person employed or engaged by the Supplier (or by a Subcontractor) violates any OHS Requirement, the Supplier shall:

(a) ensure that the violation is promptly resolved;

(b) ensure the violation is promptly and appropriately reported to the City and to the applicable competent authorities (if and to the extent required by the OHS Requirements);

(c) promptly take all reasonable steps necessary to avoid recurrence of the violation;

(d) communicate to the City its plan to avoid recurrence of the violation; and

(e) without prejudice to the foregoing Section 6.3(c), promptly remove any person responsible for the violation from the provision of the Supply if reasonable to do so or if requested to do so by the City.

6.4 Covenants Regarding the Environment

(a) The Supplier shall:

(i) at all times, be conscious of the importance of the protection of the natural, physical and biological environment at and in the vicinity of the Sites;

(ii) conduct, and cause its Representatives to conduct, their respective activities that relate to the Supply in a manner that shall have the least possible adverse effect on the natural environment and in compliance with all Environmental Laws and Consents, all at the Supplier's expense;

(iii) perform the Supply with the least degree of environmental degradation during and as a result of such performance; and

(iv) without restricting the generality or application of any other provisions of this Agreement, comply, and cause its Representatives to comply, with all applicable

Laws and Consents and with all plans and instructions contained in this Agreement or as may be reasonably issued in writing by the City concerning the existence, Release, removal, handling, transport, storage, disposal and treatment of any Hazardous Substances or other materials that are or may be hazardous to the life or health of any person or that endanger the environment or that are regulated by applicable Law.

(b) During the term of this Agreement, the Supplier shall not bring or store or permit to be used at any Site, any Hazardous Substances unless such Hazardous Substances are (i) reasonably required to carry out the Supply, and (ii) brought or stored or permitted to be used at any Site in compliance with all Laws (including Environmental Laws). The Supplier shall not Release nor permit the Release of any Hazardous Substances into the environment. The Supplier is solely responsible for all Hazardous Substances introduced to the Sites or the environment by the Supplier or its Representatives or Subcontractors, and the Supplier shall promptly and fully remediate, to the City's satisfaction, any release of Hazardous Substances on or from any Site, or in the vicinity of any Site.

6.5 Further Covenants Regarding the Sites

The Supplier shall:

(a) at its sole cost, keep any portion of any Site used in connection with the Supply in a safe and tidy condition and to maintain and operate the Supplier's equipment in a good, workmanlike and safe manner; and

(b) not to do anything at any Site which is or may become a nuisance, danger or disturbance to the City or to any other occupants or users of the Site or adjacent areas or to any works or structures or installations thereon.

6.6 Covenants Against Encumbrances

(a) The Supplier shall keep each Site and the goods included in the Supply, and each part thereof, free of all Encumbrances filed pursuant to any Law or otherwise in respect of any such work or materials. In any event, if any Encumbrance has been filed in relation to the Site or any improvement thereon, or in relation to any goods included in the Supply, the Supplier shall cause any such Encumbrance to be discharged within 30 days after the Encumbrance has come to the notice of the Supplier.

(b) The Supplier acknowledges and agrees that, in the event the Supplier fails to discharge any Encumbrance contemplated in Section 6.6(a) within 60 days of written notice of such Encumbrance being given by the City, in addition to any other right or remedy, the City may, but shall not be obligated to, discharge the Encumbrance by paying to the applicable Competent Authority, the amount claimed to be due or the amount due, together with a reasonable amount for costs and the amount paid by the City shall be paid by the Supplier to the City forthwith upon demand. In no case shall the City be required to investigate the validity of the Encumbrance prior to discharging the same in accordance with this Section 6.6(b).

6.7 Absence of Conflicts of Interest

(a) To the best of the Supplier's knowledge, after carrying out reasonable due diligence, neither the Supplier, nor any of its Representatives has given or shall give or offer to give to the City or any official, officer, employee or agent of the City any gratuity, reward, advantage or benefit of any kind as consideration for doing or forbearing to do, or for having done or forborne to do, any act in connection with this Agreement.

(b) To the best of the Supplier's knowledge, after carrying out reasonable due diligence, the Supplier, its Subcontractors, and their respective directors, officers, employees and agents have no pecuniary interests or any other current or past interests or dealings, including with any officials, officers or employees of the City, that would cause any conflict of interest or be seen to cause a conflict of interest in respect of the Supply. Should such a conflict or reasonably perceived conflict arise during the term of this Agreement, the Supplier shall declare it immediately in writing to the City. The City may direct the Supplier to resolve any conflict or perceived conflict to the reasonable satisfaction of the City. To the best of the Supplier's knowledge, the Supplier warrants that neither the Supplier nor any of its Subcontractors, or any of their respective directors, officers, employees or agents, has any predisposition, affinity or association with any third party which would materially impair or be reasonably seen to materially impair or qualify the Supplier's provision of the Supply.

ARTICLE 7
PERSONNEL

7.1 Separate Personnel

(a) It is the intention of the Parties that any personnel utilized or supplied by the Supplier hereunder shall remain employees of the Supplier for the purposes of any applicable Law and no activity performed by such personnel shall be deemed to create or imply any employment or other like relationship between such personnel and the City. If contrary to this intention such personnel are treated as employees of the City for the purposes of any applicable Law, the Supplier shall indemnify the City against any loss, cost, expense, complaint, claim, levy, assessment, penalty or fine (including any Tax liability) resulting therefrom.

(b) Neither the City nor the Supplier shall, and the Supplier shall ensure that none of its Representatives shall, induce any employee of the other, who may work in connection with the Supply, to leave his or her current employer, and neither of them shall, and the Supplier shall ensure that none of its Representatives or Subcontractors shall, employ or make an offer of employment to any such employee of the other during the term of this Agreement or the period of 365 days after the termination of this Agreement without the express prior approval in writing of the employee's current employer.

(c) If any persons are brought by the Supplier into Canada for purposes of the Supply, the Supplier shall be responsible for all immigration matters, and for the expatriation and repatriation of such personnel, and the costs of the same shall be deemed included in the Contract Price.

7.2 Changes in Personnel

The City may request the removal or replacement of any personnel engaged by the Supplier or any Subcontractor in relation to any part of the Supply, provided that such request is reasonable and made in writing stating the City's detailed reasons. The Supplier shall comply with such request as soon as reasonably practicable and shall bear the cost of replacement where the City is of the opinion that the personnel in question are guilty of misconduct, do not have acceptable qualifications or are otherwise unable or unfit to perform satisfactorily and safely as reasonably determined by the City. If the City requests a replacement for a reason other than the immediately aforementioned reasons, the City shall reimburse the Supplier its reasonable properly incurred costs of replacement.

7.3 Key Project Personnel

(a) Where there are Key Project Personnel the Supplier shall:

(i) use commercially reasonable endeavours to retain Key Project Personnel for the duration of the provision of the Supply;

(ii) take reasonable steps to ensure that Key Project Personnel dedicate a sufficient amount of their time to provide the Supply (unless otherwise agreed or approved by the City in writing);

(iii) promptly inform the City should any of the Key Project Personnel leave, or give notice of an intention to leave the Supplier, and obtain a substitute or substitutes;

(iv) not reassign or allow the reassignment of the Key Project Personnel to other projects to the material detriment of the City in providing the Supply in accordance with and during the term of this Agreement without the City's prior written consent (such consent not to be unreasonably withheld or delayed); and

(v) take all reasonable steps to ensure that the Key Project Personnel perform their roles and responsibilities in accordance with any organisational structure agreed in writing between the Parties.

(b) If:

(i) the Supplier wishes to reassign or to replace an individual designated as Key Project Personnel; or

(ii) an individual designated as Key Project Personnel gives notice of his or her intention to leave or is otherwise no longer able to perform the duties, including for reasons of illness, injury or personal hardship,

the Supplier shall provide a substitute with experience and qualifications equivalent or greater than the Key Project Personnel to be replaced, and shall provide documentation to the City to establish such experience and qualifications.

(c) Key Project Personnel who are reassigned to other work shall, to the extent possible, remain available to the project team until completion of the Supply.

(d) All the Supplier's Key Project Personnel must be fluent in both spoken and written English, except as may be agreed to the contrary between the City and Supplier in relation to specific individuals or positions to be filled from time to time.

ARTICLE 8
REPORTING

8.1 Progress Reports

(a) Monthly reports shall be prepared by the Supplier and submitted to the City in a format reasonably requested by the City including MS Word, Excel, MS Project or SmartSheet, each within seven days after the last day of the month to which it relates. From the Commissioning of the first component of the Supply (except for any period for which Section 12.2(d) is applicable), unless the City requests otherwise, acting reasonably, the format of the monthly report shall comply in form and substance with the format set out in Schedule A – Appendix 1 (Format of Report required by 8.1(a) and 8.1(b)).

(b) Each such monthly report shall include (as a minimum):

(i) status, issues and risks relating to in-progress components of the Supply with colour coding to indicate red for high risk/concern, yellow for medium risk/concern or green for no/low risk or concern;

(ii) progress report;

(iii) City spend;

(iv) update on delivery as/if required; and

(v) any other information required by the City, acting reasonably, that relates to one or more components of the Supply.

(c) In addition to the above, the Supplier will deliver other reports described in Schedule A (Scope of Goods and Services) at the times specified therein.

8.2 Assistance regarding Reporting Requirements

The Supplier shall, and shall cause its Representatives to, provide the City with reasonable assistance and information which is necessary to enable the City to comply with any Law.

ARTICLE 9
PAYMENT; AUDITS

9.1 Payment to the Supplier

(a) Subject to ARTICLE 12 and Section 9.3, the City shall pay the Supplier for the Supply in accordance with Schedule B (Prices for Supply), Schedule G (Terms and Conditions Relating to Software) and Schedule H (Terms and Conditions Relating to O&M) following the receipt of invoices prepared and delivered in accordance with Section 9.2(b) and Section 9.3 provided the Supply is accepted by the City in writing or is deemed to have been accepted by the City in accordance with Section 3.12(b).

(b) Notwithstanding any other provision hereof, prior to making any payment under this Agreement, the City may determine whether the *Builders Lien Act* (British Columbia) applies to this Agreement and, if so:

(i) payments made under this Agreement shall be subject to ten percent withholding, in the form of a lien holdback, to be held by the City in accordance with the provisions of the statute; and

(ii) the lien holdback shall be released by the City 56 days after the issuance of a certificate of completion in conformity with the *Builders Lien Act* (British Columbia)) in relation to the Supply if no liens then exist.

(c) If any lien claim based on the provisions of the *Builders Lien Act* (British Columbia) relating directly or indirectly to this Agreement exists at any time, the Supplier agrees to immediately take steps necessary or required to remove, cancel and dismiss such lien and until such lien is removed, cancelled or dismissed (as appropriate, to the satisfaction of the City), or all further payments under this Agreement may be withheld by the City or, at the discretion of the City, amounts payable to the Supplier may be used by the City to obtain the removal, cancellation or dismissal of any such lien.

(d) Unless otherwise expressly stated in the schedules hereto, the Supplier shall pay any and all costs, including freight, marine and transit insurance, Taxes, and transportation and delivery charges on all equipment or things of whatsoever nature provided by the Supplier as required by it for the purposes of the Supply and any other incidental costs and all such costs shall be deemed to be included in the Contract Price. This subsection shall supersede any other conflicts or inconsistency provision herein to the contrary.

(e) The Supplier shall be deemed to have satisfied itself as to the correctness and sufficiency of Schedule B (Prices for Supply) and to have obtained all information and to have taken into account all circumstances, risks and other contingencies that may affect the cost of performing the Supply (including any circumstances, risks or contingencies that a contractor exercising Good Industry Practice would typically expect to encounter) and any other obligation under this Agreement. The Supplier shall not be entitled to any additional compensation beyond the Contract Price (including without limitation for escalation in the prices of goods, materials and labour) except as otherwise expressly stated in this Agreement.

(f) Notwithstanding any other provisions of this Agreement, the Supplier shall not be entitled to payment for any Supply that has not been performed in compliance with the provisions of this Agreement.

9.2 Purchase Orders; Timing and Content of Invoices

(a) The City shall from time to time issue purchase orders to the Supplier in relation to the Supply. These shall not have the effect of amending or waiving the application of any provision of this Agreement.

(b) Supplier shall invoice the City the applicable amounts described in Section 9.1(a) in accordance with the following milestones provided that the Supply to which an invoice applies is Delivered or otherwise completed and accepted by the City in writing or is deemed to have been accepted by the City in accordance with Section 3.12(b):

(i) at Delivery, Supplier shall invoice the City 100% for all physical goods that are a component of the Supply provided by Supplier or its Subcontractors, including any original equipment manufacturer extended warranties purchased by the City;

(ii) at Mechanical Completion, Supplier shall invoice the City 90% for all project services rendered by Supplier or its Subcontractors in connection with the Supply (other than those services described in Schedule G (Terms and Conditions Relating to Software) and Schedule H (Terms and Conditions Relating to O&M));

(iii) upon Commissioning, Supplier shall invoice the City for:

(A) the remaining 10% for all project services rendered by Supplier or its Subcontractors in connection with the Supply (other than those services described in Schedule G (Terms and Conditions Relating to Software) and Schedule H (Terms and Conditions Relating to O&M));

(B) commissioning fees and upfront software licensing fees and credit card terminal fees, if applicable, for each Charging Unit (as such term is defined in Schedule H (Terms and Conditions Relating to O&M)) for a pro-rated portion of a 5-year term as provided in Schedule G (Terms and Conditions Relating to Software);

(C) upfront subscription fees, if applicable, for each O&M Plan Option B for each Charging Unit (as such term is defined in Schedule H (Terms and Conditions Relating to O&M)) for a pro-rated portion of 5-year term as provided in Schedule H (Terms and Conditions Relating to O&M); and

(D) upfront subscription fees, if applicable, for each O&M Plan Option C for each Charging Unit (as such term is defined in Schedule H (Terms and Conditions Relating to O&M)) for a pro-rated portion of 5-year term as provided in Schedule H (Terms and Conditions Relating to O&M); and

(E) in accordance with the invoicing provisions of Schedule H (Terms and Conditions Relating to O&M) other than amounts already invoiced in accordance with this Section 9.2.

(c) Each of the Supplier's invoices shall set out, as a minimum (and in such form or format as required by the City):

(i) the City purchase order number(s) relating to the particular Supply to which the invoice relates;

(ii) an itemized list of the amounts owing;

(iii) the invoice date and the time period to which the invoice relates;

(iv) a description of the portion of the Supply to which the invoice relates;

(i) the total amounts payable under the invoice and details of any applicable taxes including, without limitation, applicable PST and GST as separate line items;

(ii) Supplier's GST registration number;

(iii) all supporting documentation relating to disbursements;

(iv) if (A) any Subcontractor performing services relating to the Supply is not contracted by Supplier or (B) if any portion of the fees billed by Supplier with respect to any portion of the Supply requires the City to withhold Taxes in accordance with Section 16.3, then, in each case, Supplier shall provide a separate line item for such portion of the fees to enable the City to withhold Taxes on such portion of fees in accordance with applicable Canadian tax Laws; and

(v) such other information as the City may require from time to time.

(d) Any terms or conditions proposed by the Supplier to govern the Supply that are contained in any invoice (or in any shipping document, packing list or similar document) are void and of no effect, notwithstanding any statement in such document concerning the means by which the City may accept or be deemed to accept such terms or conditions.

9.3 Procedure for Invoices

(a) The Supplier shall address each of its invoices to the City, Attention: Accounts Payable, and email it to APInvoice@vancouver.ca, or to such other address as is specified in an applicable purchase order. The City shall thereafter pay the invoice within 30 days, provided the other requirements of this Agreement have been satisfied and subject to the other provisions hereof.

(b) The City shall not be liable for any interest on any invoice amount in respect of any period for any reason.

(c) The City expects to make payments by electronic funds transfer and the Supplier shall provide banking information to the City to enable it to do so.

(d) Upon receipt of a Supplier invoice that complies with the terms of this Agreement, the City will pay such invoice no later than thirty (30) days after the date of receipt of the invoice except with respect to charges then under reasonable and good faith dispute as evidenced in writing promptly sent by City to Supplier prior to the end of the thirty (30) day payment period.

9.4 Currency of Payment

All currency amounts stated herein are denominated in, all invoices hereunder shall be stated in, and all payments hereunder shall be made in, Canadian dollars.

9.5 Contested Claims for Payment

If any item contained in an invoice submitted by the Supplier is contested by the City, the City shall give prompt notice thereof, together with reasons to the Supplier.

9.6 Audits

(a) The Supplier shall maintain up-to-date records and accounts which clearly document the provision of the Supply and shall make the same available to the City upon request. The City may request copies of all such records and accounts which shall be provided to the City by the Supplier (subject to reimbursement of the Supplier's reasonable copying costs and any other direct costs and expenses, if any) at any time prior to the expiry of 365 days after completion of all of the Supply or earlier termination of this Agreement. For avoidance of doubt, any records and accounts provided by the Supplier in accordance with this Section 9.6(a) shall be deemed to be Confidential Information;

(b) Not later than three years after the completion of all of the Supply or earlier termination of this Agreement, the City can itself, on notice of not less than 14 days, require that a firm of accountants, surveyors or other auditors nominated by it audit any such records and accounts of the Supplier. For avoidance of doubt, any records and accounts or other documents provided by the Supplier in accordance with this Section 9.6(b) shall be provided only subject to the accountants, surveyors or other auditors, and each of them, being subject to and agreeing to meet such of the Supplier's reasonable requirements as to confidentiality as the Supplier deems (at its sole discretion) to be appropriate in the circumstances; and

(c) Any overpayments by the City discovered during the course of any such audit pursuant to Section 9.6(b)shall be payable by the Supplier to the City within 30 days of such discovery, and if the overpayments have been caused by an act or omission of the Supplier and the amount of those overpayments is no less than one quarter of the total amount paid by the City to the Supplier in respect of the Supply, then the costs of the relevant audit shall be for the account of the Supplier.

9.7 Set Off

Notwithstanding any provision to the contrary in this Agreement and without prejudice to any other remedy which the City may have (whether in common law or equity), the City shall be entitled to deduct from and set off against any sum(s) otherwise due to the Supplier hereunder any sums which

are due from the Supplier to the City or which the Supplier is liable to pay to the City under this Agreement or in connection herewith (including without limitation any monies overpaid to the Supplier under this Agreement or otherwise due and payable to the City by reason of any error in payment under this Agreement).

ARTICLE 10
CERTAIN ADDITIONAL OBLIGATIONS OF THE CITY

10.1 Scheduled Items

The City shall make available, free of cost and without delay or in accordance with any agreed timetable or Schedule A (Scope of Goods and Services) to the Supplier for the purpose of the Supply, the personnel, equipment, facilities, services (including services of third parties) and information described in such Schedule A (Scope of Goods and Services).

10.2 Other Information

The City shall, within a reasonable time following a written request by the Supplier, provide to the Supplier free of cost such further information, which the City considers relevant to provision of the Supply and which is either already in its possession or reasonably within its power to obtain.

10.3 Decisions in Writing

On all matters properly referred to it in writing by the Supplier, the City shall (wherever practicable) give its decision in writing within a reasonable time having regard to the Time(s) for Completion and the Supplier's obligations with regard to the Supply.

10.4 Access to the Site

Except to the extent prohibited by applicable Law or any Consent, the City shall grant to the Supplier and its Subcontractors non-exclusive, timely and in accordance with any agreed schedule, access (as the City is reasonably able to provide) to all necessary areas of the Site on and from the Effective Date and such other non-exclusive access as is necessary or appropriate to perform the Supply and the Supplier's and its Subcontractor's other obligations in accordance with this Agreement.

ARTICLE 11
LIABILITY AND INSURANCE

11.1 Covenants of Indemnification by the Supplier

(a) The Supplier shall indemnify and keep indemnified and hold the City, the Other City Entities and their respective officials, officers, employees and agents harmless against all losses, liabilities, claims, demands, costs and expenses (including legal fees), fines, penalties and charges (including those imposed by statute or otherwise imposed), actually incurred and arising out of or in connection with, or consisting of:

(i) any:

(A) damage to a Site or any part thereof, or any property whether located at a Site or otherwise, which occurs during the provision of the Supply;

(B) any claim by a Subcontractor under the *Builders Lien Act* (British Columbia);

(C) damage to the natural environment, including any remediation cost recovery claims;

(D) loss or damage arising from a claim by any third party or by any employee or Subcontractor of the Supplier, in each case, concerning or arising out of the Supply;

(E) occupational illness, injury or death of any person, whether at a Site or otherwise, which occurs during, or as a result of, the provision of the Supply;

(F) failure by the Supplier to fully comply with the provisions of this Agreement; provided that for clarity, no such indemnity claim shall be commenced until the expiration of any applicable cure period provided herein;

(G) breach by the Supplier or any Subcontractor of any Law in the course of, or as a result of, the provision of the Supply;

(H) actual or alleged infringement of any Intellectual Property Rights caused by the provision of the Supply or the use of any process, work, material, matter, thing or method used or supplied by the Supplier or any Subcontractor in the provision of the Supply; or

(I) breach of the warranties of the Supplier contained herein,

in each case to the extent that it is due to an act, omission or default, or any breach of Law or this Agreement, of the Supplier, a Subcontractor or any Representative of the Supplier or any employee, agent or contractor of any of them; or

(ii) any defect in a good, work or material provided as part of the Supply or any failure of any such good, work or material to function safely or to satisfy any applicable safety standard, in each case to the extent that it is due to an act, omission or default, or any breach of Law or this Agreement, of the Supplier, a Subcontractor or any Representative of the Supplier or any employee, agent or contractor of any of them; provided that (A) notwithstanding Supplier's indemnity in this section, Supplier is entitled to charge and invoice the City for, and the City agrees to pay Supplier, the amounts for the goods and services to be supplied by Supplier under the terms of Schedule H (Terms and Conditions Relating to O&M) and (B) for clarity, no such indemnity claim shall be commenced until the expiration of any applicable cure period provided herein.

(b) Nothing in this Section 11.1 nor otherwise in this Agreement shall limit or exclude any direct liability (whether in contract, tort, for breach of statutory duty or any other legal basis) of the Supplier to any person, including without limitation any liability for:

(i) the Supplier's default hereunder or fraud, fraudulent misrepresentation or reckless misconduct in the provision of the Supply; or

(ii) any loss or damage flowing from the termination of this Agreement.

(c) The Supplier appoints the City as the trustee of the Other City Entities and of their and the City's officials, officers, employees and agents in relation to the covenants of

indemnification of the Supplier contained in this Section 11.1 and the City accepts such appointment.

11.2 Contamination of Lands

Without limiting any other provision hereof or any other remedy available to the City hereunder, the Supplier agrees and covenants that if, at any time during the term or following the expiry of this Agreement, the Site or any other lands affected by the Supply are found to be contaminated or polluted (as determined pursuant to Environmental Laws) as a result of or in connection with the Supply, the Supplier shall forthwith at its sole cost:

(a) undertake all necessary audits, investigations, tests and surveys to determine the nature and extent of the contamination or pollution;

(b) notify the City of the nature and extent of the contamination or pollution and any proposed or required work necessary to control, abate, dissipate or remove (as appropriate) the pollution or contamination as required by Environmental Laws; and

(c) to the extent it is possible to reasonably attribute the cause of contamination or pollution to the Supplier or any of its Subcontractors, undertake only such work referred to in the foregoing paragraph (b) that rectifies the contamination or pollution caused by the Supplier.

11.3 Site Diligence

Notwithstanding Section 11.2, each Party shall provide any relevant information to the other Party and work together in good faith to conduct any diligence reasonably required at any Site prior to commencement of any work by Supplier or its Subcontractor in respect of providing the Supply at a Site (including, without limitation, agreement on costs related to any such diligence or pre-emptive remediation, if applicable).

11.4 Conduct of Claims

In the event of any claims, statutory fees, costs, charges, penalties (including without limitation any legal costs), contributions, compensations, cost recoveries, expenses or fines being levied or claimed from a person in respect of which an indemnity is provided by the Supplier pursuant to ARTICLE 11, the following provisions shall apply:

(a) subject to Sections 11.4(b), 11.4(c) and 11.4(d), where a person is or may be entitled to indemnification from the Supplier in respect of all (but not part only) of the liability arising out of a claim, such person entitled to indemnification may at its sole election and subject to:

(i) approval by any relevant insurers (without prejudice to Section 11.4(f)); and

(ii) the Supplier providing the party entitled to indemnification with a secured indemnity to its reasonable satisfaction against all costs and expenses (including legal expenses) that it may incur by reason of such action,

permit or require the Supplier to dispute the claim on behalf of the person entitled to indemnification at the Supplier's own expense and take conduct of any defence, dispute, compromise, or appeal of the claim and of any incidental negotiations; provided that the person entitled to indemnification shall give the Supplier (provided at the Supplier's cost) all reasonable cooperation, access and assistance for the purposes of considering and resisting such claim;

(b) with respect to any claim conducted by the Supplier pursuant to Section 11.4(a):

(i) the Supplier shall keep the person entitled to indemnification fully informed and consult with it about material elements of the conduct of the claim;

(ii) the Supplier shall not bring the name of the person entitled to indemnification (or any Group Member thereof) into disrepute; and

(iii) the Supplier shall not pay or settle such claims without the prior consent of the person entitled to indemnification, such consent not to be unreasonably withheld or delayed;

(c) a person entitled to indemnification shall be free to pay or settle any claim on such terms as it thinks fit (and without prejudice to its rights and remedies under this Agreement) if:

(i) the Supplier is not entitled to take conduct of the claim in accordance with Section 11.4(a); or

(ii) the Supplier fails to comply in any material respect with the provisions of Sections 11.4(a) or 11.4(b);

(d) the person entitled to indemnification pursuant to ARTICLE 11 shall be free at any time to give notice to the Supplier that it is retaining or taking over (as the case may be) the conduct of any defence, dispute, compromise or appeal of any claim (or of any incidental negotiations) to which Section 11.4(a) applies. On receipt of such notice the Supplier shall promptly take all steps necessary to transfer the conduct of such claim to the person entitled to indemnification, and shall provide to the person entitled to indemnification all reasonable co-operation, access and assistance for the purposes of considering and resisting such claim;

(e) if the Supplier pays to the person entitled to indemnification an amount in respect of an indemnity and the person entitled to indemnification subsequently recovers (whether by payment, discount, credit, saving, relief or other benefit or otherwise) a sum which is directly referable to the fact, matter, event or circumstances giving rise to the claim under the indemnity, the person entitled to indemnification shall forthwith repay to the Supplier whichever is the lesser of:

(i) an amount equal to the sum recovered (or the value of the saving or benefit obtained) less any out-of-pocket costs and expenses (including legal expenses) properly incurred by the person entitled to indemnification in recovering the same; and

(ii) the amount paid to the person entitled to indemnification by the Supplier in respect of the claim under the relevant indemnity,

provided that there shall be no obligation on the part of the person entitled to indemnification to pursue such recovery and that the Supplier is repaid only to the extent that the amount of such recovery aggregated with any sum recovered from the Supplier exceeds any loss sustained by the person entitled to indemnification;

(f) the Supplier shall inform the person entitled to indemnification of the requirements of any insurer who may have an obligation to provide an indemnity in respect of any liability arising under this Agreement and in relation to such the person entitled to indemnification shall issue instructions accordingly; and

(g) any person entitled to an indemnity from the Supplier must take all reasonable measures to mitigate any loss, damage or liability that it may suffer in respect of any such matter.

11.5 Insurance

The Supplier will comply with the requirements of Schedule L – Appendix 1 (Insurance Requirements and Certificates).

11.6 Liability Disclaimer and Limitation of Liability

Notwithstanding anything in this Agreement to the contrary:

(a) NEITHER PARTY NOR THEIR REPRESENTATIVES OR SUBCONTRACTORS WILL BE LIABLE TO THE OTHER PARTY OR ITS REPRESENTATIVES FOR ANY INDIRECT OR CONSEQUENTIAL (INCLUDING LOST PROFIT), INCIDENTAL, SPECIAL, PUNITIVE, OR EXEMPLARY DAMAGES, WHETHER OR NOT RELATED TO SUCH PARTY'S OR ITS REPRESENTATIVES' OR SUBCONTRACTORS OWN NEGLIGENCE SAVE AND EXCEPT WHERE (1) A PARTY HAS COMMITTED FRAUD, WILFUL MISCONDUCT OR GROSS NEGLIGENCE IN RESPECT OF ANY OF ITS RIGHTS OR OBLIGTIONS UNDER THIS AGREEMENT, AND (2) SUPPLIER HAS BREACHED ITS OBLIGATIONS RELATING TO PRIVACY AND DATA SECURITY UNDER THIS AGREEMENT.

(b) Save and except if Supplier has committed fraud, wilful misconduct or gross negligence in respect of any of its rights or obligations under this Agreement, Supplier's aggregate liability for any damages claims relating to or in connection with this Agreement shall not exceed the limits of insurance coverage in the applicable insurance policies required in Schedule L – Appendix 1 (Insurance Requirements and Certificates) relating to the applicable damages claim asserted, and such limits shall apply whether or not Supplier's insurance covers the damages; provided that Supplier's aggregate liability for all damages under this Agreement of any nature shall not exceed Ten Million Dollars ($10,000,000).

(c) Save and except if the City has committed fraud, wilful misconduct or gross negligence in respect of any of its rights or obligations under this Agreement, the City's aggregate liability for any damages claims relating to or in connection with this Agreement shall not exceed the aggregate fees paid by the City to Supplier under this Agreement in the twelve (12) months prior to the event giving rise to the damages.

(d) The limitations or exclusions in this Section 11.6 will limit or exclude such liability not only in contract but also in tort, including negligence or otherwise at law. The Supplier does not exclude or limit its liabilities to the City to the extent they may not be excluded or limited under applicable Laws.

ARTICLE 12
FORCE MAJEURE; TERMINATION

12.1 Force Majeure

(a) Neither Party nor Supplier Guarantors shall be deemed to be in breach of this Agreement or otherwise liable to the other Party in any manner whatsoever for any failure or delay in performing its obligations under this Agreement reasonably due to Force Majeure; provided that the foregoing shall not apply to either Party's or any Supplier Guarantor's inability to perform due to its inability to meet any payment or other financial obligations.

(b) If either Party's or a Supplier Guarantor's performance of its obligations under this Agreement is affected by an event of Force Majeure, then:

(i) it shall give written notice to the other Party, specifying the nature and extent of the event of Force Majeure, the anticipated consequences resulting from such Force Majeure, and submit a specific plan that endeavors to minimize and mitigate those consequences, within ten days after becoming aware of the event of Force Majeure;

(ii) performance of such obligation(s) shall be deemed suspended but only for a period equal to the delay reasonably caused by such event, plus a reasonable time required to recommence such Party's performance in accordance with this Agreement;

(iii) it shall not be entitled to payment from the other Party or a Supplier Guarantor in respect of extra costs and expenses incurred by virtue of the event of Force Majeure;

(iv) the Time(s) for Completion shall be extended to take into account such delay; and

(v) within five days of the cessation of any Force Majeure event, the Party or Supplier Guarantor affected thereby shall submit a written notice to the other Party, specifying the actual duration of the delay of its obligations caused by the event of Force Majeure and the consequences resulting from such delay, and submit a specific plan to minimize and mitigate those consequences.

(c) The affected Party or the Supplier Guarantors shall use all reasonable diligence in accordance with Good Industry Practice to mitigate the cause and the result of an event of Force Majeure and to remedy the situation and resume its obligations under this Agreement, including complying with any instructions from the City, as to how to do so.

(d) Notwithstanding the obligations of a Party or Supplier Guarantor affected by an event of Force Majeure pursuant to Sections 12.1(b) and 12.1(c), if the event of Force Majeure renders it impossible or impractical for the Supplier or a Supplier Guarantor to provide the Supply in accordance with this Agreement for a period of at least 60 consecutive days, either Party or Supplier Guarantors may terminate this Agreement upon notice delivered to the other Party at any time following the expiration of such period of 60 consecutive days.

12.2 City Suspension and Termination Rights

The City shall have the following rights:

(a) The City may order the suspension of all or part of the Supply at any time and for such period as it determines, by notice with immediate effect to the Supplier, in the event of a Safety Incident; and upon receipt of any such notice of suspension, the Supplier shall immediately cease performing the Supply, minimise expenditure and comply with any reasonable instructions of the City relating to such Safety Incident, including any investigations.

(b) If the City reasonably considers that the Supplier is not discharging any of its material obligations under this Agreement, the City may inform the Supplier by written notice stating the grounds for the notice. If Supplier fails to cure such breach or to commence and diligently and continuously take commercially reasonable steps to cure such breach

within thirty (30) days (provided that in the latter case Supplier shall have no more than sixty (60) days by which to cure a breach) following Supplier's receipt of such written notice (or such longer period as agreed by the Parties), the City may by a further notice to the Supplier of at least fourteen (14) days terminate this Agreement.

(c) In recognition that the Supplier's collection, storage, use and protection of Personal Information in material compliance with Applicable Privacy Laws and the terms of this Agreement relating to privacy and data security is a material condition of this Agreement, the City may, at its option, terminate this Agreement on at least fourteen (14) days prior written notice to the Supplier if:

(i) Supplier is not in material compliance with Applicable Privacy Laws and the terms of this Agreement relating to privacy and data security and the Supplier fails to cure such breach within thirty (30) days of: (A) becoming aware of such breach (or when Supplier reasonably should have been aware) or (B) following receipt of written notice of such breach by the City, or

(ii) (A) any of the circumstances set out in Section 15.1(a) change during the term of this Agreement and, as a result of such change, the Supplier is required to comply with FOIPPA and, (B) following a period of at least sixty (60) days after the date of determination that Supplier must comply with FOIPPA, provided Supplier is diligently and continuously during such period is taking steps to comply with FOIPPA, the City is not satisfied, acting reasonably, that the Supplier is able to comply with FOIPPA.

(d) In recognition that Supplier's material compliance with its obligations under Schedule D (PCI Requirements) is a material condition of this Agreement, the City may, at its option, exercise one of more if the following rights if Supplier is in breach of its obligations under Schedule D (PCI Requirements) and fails to cure such breach within thirty (30) days of: (A) becoming aware of such breach (or when Supplier reasonably should have been aware) or (B) following receipt of written notice of such breach by the City:

(i) suspend, for a period of time reasonably determined by the City, this Agreement on at least fourteen (14) days prior written notice to the Supplier in which case Supplier shall reimburse the City, at the end of the suspension period, fees paid by the City under Schedule G (Terms and Conditions Relating to Software) and Schedule H (Terms and Conditions Relating to O&M) on a pro-rata basis based on the length of time the Agreement was suspended,

(ii) direct Supplier, on at least fourteen (14) days prior written notice, to continue operating the Charging Stations (as such term is defined in Schedule G (Terms and Conditions Relating to Software)) without charge to Customers (as such term is defined in Schedule G (Terms and Conditions Relating to Software)), in which case Supplier shall reimburse the City, on a monthly basis, the documented cost of energy for Charging Sessions (as such term is defined in Schedule G (Terms and Conditions Relating to Software)) at such Charging Stations, or

(iii) terminate this Agreement on at least fourteen (14) days prior written notice to Supplier.

(e) The City may terminate this Agreement with immediate effect if:

(i) the Supplier becomes bankrupt or insolvent, goes into liquidation, has a receiver or administrator appointed over it or any of its assets of undertaking, enters into any arrangement for the benefit of its creditors, becomes the subject of any

moratorium or carries on business under a receiver, trustee, manager or arrangement for the benefit of its creditors, or if any act is done or event occurs which (under applicable Laws) has a similar effect to any of these acts or events; or

(ii) a Change in Control of the Supplier occurs and the City reasonably considers that the Change in Control shall substantively affect the Supplier's ability to perform its obligations under this Agreement.

12.3 Supplier Suspension and Termination Rights

Supplier shall have the following rights:

(a) If a Supplier invoice that complies with the terms of this Agreement is delivered to the City in respect of services supplied under Schedule G (Terms and Conditions Relating to Software) or Schedule H (Terms and Conditions Relating to O&M) is thirty (30) days or more overdue after the initial thirty (30) day payment period set out in Section 9.3(d) (except in respect of charges then under reasonable and good faith dispute), Supplier may, on a further fourteen (14) days advance written notice to the City, suspend or terminate some or all of the services supplied under the applicable Schedule to which the unpaid invoice relates until the overdue amounts are paid in full. Upon any such suspension or termination, all rights in the Software or O&M services, as applicable, granted to City shall automatically revert to Supplier, and City shall have no further rights in, and shall immediately cease all use of, the Software or O&M services, as applicable.

(b) Supplier and Supplier Guarantors shall have the right to terminate this Agreement on at least fourteen (14) days prior written notice to the City if Supplier or Supplier Guarantors determine, in their reasonable judgment supported by credible evidence, that the City is in breach of any applicable anti-bribery or anti-money laundering Laws, Supplier has given written notice to the City of such breach and relevant details of the credible evidence of breach, and the City fails to (i) cure the breach, or (ii) provide information demonstrating compliance with such Laws, within thirty (30) days of receiving written notice of breach from Supplier. Nothing in this Agreement shall require a Party or Supplier Guarantors to perform any part of this Agreement or take any actions if, by doing so, the Party or Supplier Guarantors would not comply with applicable Laws.

12.4 Consequences of Termination

The following consequences shall apply upon a termination:

(a) On termination of this Agreement for any reason, the Supplier shall, as soon as reasonably practicable:

(i) deliver to the City all work and Documentation produced by or on behalf of the Supplier during the course of performing the Supply;

(ii) return (or destroy if otherwise directed by the City in writing) all Confidential Information provided to it for the purposes of this Agreement;

(iii) return all of the City's Site access cards, equipment and other items provided under this Agreement, failing which, the City may enter the relevant premises and take possession thereof, and, until any such access cards, equipment and other items have been returned or repossessed, the Supplier shall be solely responsible for its or their safe-keeping;

(iv) if so requested by the City, take reasonable steps to assign any Subcontractor contracts to the City and do all things and execute all documents necessary to give effect thereto; and

(v) otherwise comply with all reasonable requirements of the City arising from the cessation of the Supply or the continuing development of the Site.

(b) The Supplier shall be entitled to be paid its reasonable properly and documented incurred costs of compliance with Section 12.4(a) and its reasonable demobilization costs, up to a maximum of Fifteen Thousand ($15,000) Dollars, in aggregate, save in circumstances in which the City reasonably claims that the termination was a consequence of a Safety Incident or a default by the Supplier in the provision of any part of the Supply, in which case all such costs shall be for the Supplier's own account.

(c) On termination or suspension of this Agreement for any reason, the Supplier shall be entitled to payment for any completed portion of the Supply rendered in full compliance herewith prior to the time of termination, in accordance with Schedule B (Prices for Supply).

12.5 Other Surviving Rights and Liabilities of Parties

(a) Termination of this Agreement shall not prejudice or affect the accrued rights or claims and liabilities of the Parties (or the Supplier Guarantors).

(b) After termination of this Agreement, the provisions of Sections 3.9 and 9.6, ARTICLE 11, ARTICLE 14, ARTICLE 15 and ARTICLE 17 shall remain in force.

ARTICLE 13
ASSIGNMENT AND SUBCONTRACTING

13.1 Assignment

Neither Party shall assign, transfer, mortgage, charge or deal in any other manner with this Agreement or any of its rights and obligations under or arising out of the Agreement (or any document referred to herein), or purport to take any such action without the prior written consent of the other.

13.2 Subcontracting

(a) Save in the case of Subcontractor(s) whose role in the provision of the Supply is expressly provided for in the schedules hereto (and only to the extent so provided for), the Supplier may not subcontract any part of the Supply without the City's prior written consent.

(b) The Supplier shall not without the written consent of the City (which shall not be unreasonably withheld or delayed) initiate or terminate any contract with a Subcontractor.

(c) If the Supplier is unable to enter into a contract with a Subcontractor whose role in the provision of the Supply is expressly provided for in the schedules hereto, it shall as soon as reasonably practicable inform the City of the reason for such inability and procure the services of a replacement subcontractor that is acceptable to the City, acting reasonably.

(d) The Supplier shall be responsible for the acts, defaults or neglect or any omission of each Subcontractor, its employees and agents in all respects as if they were the acts and defaults or neglect or omission of the Supplier its employees or agents themselves.

ARTICLE 14
INTELLECTUAL PROPERTY

14.1 Assignment

The Supplier acknowledges and agrees that the City is the exclusive owner of all right, title, and interests in and to the Documentation, including, without limitation, all Intellectual Property Rights therein. The Supplier shall assign and hereby assigns to the City all right, title, and interests in and to the Documentation, including, without limitation, all existing and future Intellectual Property Rights in and to the Documentation, effective upon their creation to the fullest extent permitted by Law. Insofar as such right, title, and interest do not so vest automatically or immediately in the City by operation of law or under this Agreement, subject to Section 14.2, the Supplier holds legal title of all right, title, and interests in and to the Documentation, including, without limitation, all Intellectual Property Rights therein, in trust for the City and grants to the City an irrevocable, perpetual, fully paid-up, royalty-free, worldwide, transferable and non-exclusive licence to, itself and through contractors and agents, use, copy, amend, reproduce, modify and create derivative works of such Documentation for any purpose. Such licence shall include the right to sub licence to any third party without restriction.

14.2 Further Assistance

If and to the extent that any of the right, title, and interest in and to the Documentation, including, without limitation, all Intellectual Property Rights therein, is not assigned automatically or immediately to the City under Section 14.1, the Supplier undertakes, at the expense of the City and at any time either during or after this Agreement upon request from the City (notwithstanding that the City may do so in its own name and at its own cost), to execute all documents, make all applications, give all assistance and do all acts and things as may, in the reasonable opinion of the City, be necessary or desirable to vest all right, title, and interest in and to the Documentation, including, without limitation, all Intellectual Property Rights therein, in the City and to register them in, the name of the City and otherwise to protect and maintain such right, title, and interest. The Supplier further agrees to cooperate fully with the City both during and after the termination of this Agreement, with respect to signing further documents and doing such acts and other things reasonably requested by the City to confirm the transfer of ownership of the Documentation or to obtain or enforce patent, copyright, trade secret, or other protection for the Documentation. The Supplier shall not receive any consideration or royalties in respect of such transfer of ownership, beyond the fees, provided that the expense of obtaining or enforcing intellectual property protection shall be borne by the City.

14.3 Supplier Undertakings and Representations and Warranties

(a) The Supplier undertakes:

(i) to notify the City in writing of the full details of Documentation promptly upon its creation;

(ii) whenever requested to do so by the City and in any event on the termination of this Agreement (as provided for in ARTICLE 12), promptly to deliver to the City all correspondence, documents, papers and records on all media (and all copies or abstracts of them), recording or relating to any parts of the Documentation which are in its possession, custody or power;

(iii) that the Supplier shall not, either during the term of this Agreement or thereafter, directly or indirectly, contest, or assist any third party to contest, the City's ownership of the Documentation or of any Intellectual Property Rights related thereto, and

(iv) not to register nor attempt to register any Intellectual Property Rights in the Documentation unless requested to do so by the City.

(b) The Supplier represents and warrants to the City that:

(i) it has not given and shall not give permission to any Subcontractor or third party to use any of the Documentation, nor any of the Intellectual Property Rights in the Documentation, other than as provided for in this Agreement or otherwise in accordance with the instructions of the City;

(ii) it has not given, and shall not give, to the City, nor shall it use in the provision of the Supply, any confidential material or documents of any former client or customer of the Supplier or of any other third party, unless the Supplier has received prior written authorization to do so from the City and from the owner of the confidential material or documents;

(iii) it has the absolute right to make the assignments of the right, title, and interest in and to the Documentation contemplated in this Agreement and to grant the rights granted under this Agreement;

(iv) it is unaware of any use by any third party or any unauthorized use by a Subcontractor of any of the Documentation or any Intellectual Property Rights in the Documentation; and

(v) the use of the Documentation or the Intellectual Property Rights in the Documentation by the City shall not, to the knowledge of the Supplier, infringe any Intellectual Property Rights of any third party.

14.4 Background Intellectual Property

Notwithstanding and superseding anything to the contrary in this ARTICLE 14, each Party retains title to all Intellectual Property Rights owned or possessed by it or any of its affiliates prior to or independent of performance of this Agreement and used by it in fulfilling its obligations under this Agreement, as well as any modifications or improvements made thereto in the course of performing this Agreement (“**Background IP**”). For the avoidance of doubt, the Software, SKY™ Network, (each as defined in Schedule G (Terms and Conditions Relating to Software)), the Supplier’s mobile applications and all such other Background IP not specifically developed for the City pursuant to a mutually-agreed upon statement of work (including, in each case, any improvements, modifications or derivatives related thereto) and any Documentation relating to each of the foregoing constitute the Background IP of Supplier. To the extent that one Party acquires any right, title, or interest in and to any aspect of the modifications or improvements to the Background IP of the other Party, such first Party shall assign such right, title, and interest to the second Party, immediately following such acquisition.

14.5 Supplier Employees’ and Subcontractors’ Rights

The Supplier:

(a) warrants that the Supplier’s employees, Subcontractors and agents have waived or shall have waived in whole all moral rights (including, without limitation, any similar rights allowing the rights holder to restrain or claim damages for any distortion, mutilation, or other modification of works or any part thereof, and to restrain use or reproduction of works in any manner) they may have in the Documentation;

(b) indemnifies the City, its officers, agents, contractors and employees against any liability, cost, loss or damage (including legal costs on a solicitor-client basis) suffered or incurred that arises under any breach of the warranty contained in Section 14.5(a); and

(c) must do all things reasonably requested by the City, including signing or procuring the signature of particular forms, to give full effect to Section 14.5(a).

14.6 No Additional Remuneration

The Supplier acknowledges that, except as provided by Law, no further remuneration or compensation (beyond that expressly provided for in this Agreement) is or may become due to the Supplier in respect of the performance of its obligations under this ARTICLE 14.

ARTICLE 15
PRIVACY; DATA SECURITY; CONFIDENTIALITY

15.1 Privacy and Data Security

The City and Supplier acknowledge that they are each subject to Applicable Privacy Laws, which imposes significant obligations to protect all Personal Information that is collected, stored, used, and processed in the course of performance of this Agreement. The Supplier shall comply with these and other obligations described in Schedule E – Appendix 1 (Additional Privacy and Data Security Requirements).

(a) City and Supplier agree as follows:

(i) FOIPPA does not apply to the collection, storage, use and protection of Personal Information that is collected by the Supplier under this Agreement,

(ii) all Personal Information collected by Supplier under this Agreement is collected through, and retained within, Supplier's or one or more subcontractors' software,

(iii) Supplier's software, and the software of its subcontractors, are not integrated with, or connected to, City software or hardware,

(iv) Supplier covenants that it will not disclose any Personal Information to the City, and

(v) based on the above, the City does not have custody or control, as such terms are used in, and as is required by, FOIPPA, of any Personal Information collected by Supplier under this Agreement.

(b) City agrees that all Personal Information collected and processed under this Agreement by the Supplier is "under the custody and control" of the Supplier for the purposes of Applicable Privacy Laws.

(c) Supplier will advise all Customers (as such term is defined in Schedule G (Terms and Conditions Relating to Software)) that it has custody and control of any Personal Information of such users and to direct any questions or access to information requests to the Supplier.

15.2 No Promotion

The Supplier shall not, and shall ensure that its Subcontractors shall not, disclose or promote any relationship with the City, including by means of any oral declarations, announcements, sales literature, letters, client lists, press releases, brochures or other written materials, without, in each case, the express prior written consent of the City. The Supplier shall not use the City's logo or any of the City's official marks without the express prior written consent of the City.

15.3 Confidentiality Obligations

Each Party shall keep the Confidential Information of the other Party confidential and each Party shall not use such Confidential Information except for the purpose of exercising or performing its rights and obligations under this Agreement or where, in the case of the City, otherwise necessary to pursue the public business of the City (a "**Permitted Purpose**"), or disclose the Confidential Information in whole or in part to any third party, except as expressly permitted by this ARTICLE 15.

15.4 Disclosure to Representatives

A Party may disclose the other Party's Confidential Information to those of its Representatives and Subcontractors who need to know such Confidential Information for the Permitted Purpose, provided that it informs such Representatives and Subcontractors of the confidential nature of the Confidential Information prior to disclosure, and at all times it is responsible for such Representatives' compliance with the confidentiality obligations set out in this ARTICLE 15.

15.5 Disclosures Required by Law

A Party may disclose Confidential Information to the extent required by any applicable Laws or by any Competent Authority provided that, where legally permitted, it promptly notifies the other Party before doing so, gives the other Party a reasonable opportunity to take any steps that the Party considers necessary to protect the confidentiality of that information, and notifies the third person that the information is Confidential Information. In any event, a Party shall furnish only that portion of the Confidential Information which it is legally required to disclose and shall use its reasonable endeavours to obtain a protective order or other reliable assurance that the Confidential Information shall be accorded confidential treatment.

15.6 Other Disclosures by the City

Subject to Section 15.5, the City's obligations under this ARTICLE 15 are wholly subject to and qualified by, the applicable provisions of the *Freedom of Information and Protection of Privacy Act* (British Columbia) and, notwithstanding any other provision of this ARTICLE 15, the City may disclose Confidential Information in any manner compliant with such statute or otherwise in furtherance of its public role or duties, including in the course of publicly reporting to the Vancouver City Council.

15.7 Interpretation; Enforcement and Survival

(a) Notwithstanding anything in this ARTICLE 15 to the contrary, nothing in this ARTICLE 15 shall affect the Parties' rights and obligations under ARTICLE 14.

(b) The Parties acknowledge that a breach of any of the obligations or provisions contained in this ARTICLE 15 could cause the other Party to suffer loss which may not be adequately compensated for by damages and that the other Party may, in addition to any other remedy or relief, enforce the performance of this Agreement by injunction or specific performance upon application to a court of competent jurisdiction without proof of actual or special damage and notwithstanding that in any particular case damages may

be readily quantifiable, and such breaching Party must not plead sufficiency of damages as a defence in the proceeding for such injunctive relief.

ARTICLE 16
TAXES

16.1 Taxes for Own Accounts

Unless otherwise expressly stated in this Agreement, any Taxes becoming due and payable by either Party pursuant to any applicable Laws as a result of the entering into, the performance of obligations under or the taking of payment pursuant to this Agreement, shall be for the account of that Party, and for greater certainty the Contract Price includes all such Taxes, except for applicable Taxes arising under all sales, excise and value added tax legislation (including, without limitation, the *Excise Tax Act* (Canada) and similar Canadian provincial legislation) (collectively, "**Sales Tax**") as a result of the sale of the Supply within Canada hereunder, unless it is clearly stated that they are intended to be Sales Tax-inclusive.

16.2 Supplier Representations and Covenants Regarding Taxes

(a) Supplier represents that:

(i) it has filed applicable income tax returns in Canada as required by applicable Laws;

(ii) it has Canadian employees; and

(iii) its GST/HST number is 727423113.

(b) Supplier covenants that:

(i) all portions of the Supply consisting of services physically performed in the City of Vancouver shall be provided solely by Canadian employees of Supplier;

(ii) to the extent that any portion of the Supply consisting of services physically performed in the City of Vancouver is performed by a Subcontractor, Supplier shall engage and directly contract with such Subcontractor for the provision of such services and such Subcontractor must not be a non-resident of Canada as such term is defined in applicable tax Laws of Canada; and

(iii) it will file applicable income tax returns in Canada as required by applicable Laws.

16.3 Withholding Taxes

(a) Notwithstanding any other provision to the contrary, if Supplier breaches any of the covenants in Section 16.2(b) or if the City otherwise reasonably determines that it is necessary to satisfy its obligations under any Law relating to Taxes, the City may:

(i) withhold an amount from a payment made to the Supplier; and

(ii) pay the withheld amount directly to the relevant Competent Authority.

(b) If an amount withheld in accordance with Section 16.3(a) is paid by the City to the relevant Competent Authority, it is deemed to have been paid to the Supplier on the date on which the remainder of the payment to which it relates was paid to the Supplier.

(c) The Supplier agrees and acknowledges that it has no claim against the City for any amounts properly withheld and paid to the relevant Competent Authority in accordance with Section 16.3(a).

(d) If the City does not withhold an amount under Section 16.3(a) which it is required to withhold pursuant to any Laws relating to Taxes, the Supplier agrees to pay that amount to the City, upon request by the City and the City will remit to the proper Competent Authority.

(e) The Supplier agrees that the City shall not be required to increase any payment to the Supplier by the amount withheld by the City under Section 16.3(a)

ARTICLE 17
DISPUTE RESOLUTION

17.1 Optional Procedure

All claims, disputes or issues in dispute between the City and the Supplier (or Supplier Guarantors) in relation to this Agreement shall be decided by mediation or arbitration, if the Parties so agree in writing, or, failing any such agreement, by the courts of competent jurisdiction in the Province of British Columbia.

17.2 Arbitration

In the event that Parties (including Supplier Guarantors) agree to arbitration pursuant to Section 17.1:

(a) the arbitration shall be conducted pursuant to the *Commercial Arbitration Act* (British Columbia) and shall be governed by the rules of the British Columbia International Commercial Arbitration Centre, except that the arbitrator or arbitrators shall be agreed upon by the Parties, and failing agreement by the Parties, shall be appointed by a court of competent jurisdiction within the Province of British Columbia;

(b) the Parties shall share equally the costs of the arbitration but shall be responsible for their own separate costs and expenses in relation to the arbitration including legal fees and disbursements; and

(c) the arbitration shall take place in Vancouver, British Columbia and shall be governed by the laws of British Columbia.

ARTICLE 18
MISCELLANEOUS

18.1 Time of the Essence

Time is of the essence of this Agreement, including without limitation in relation to the Time(s) for Completion.

18.2 Costs

Each of the Parties hereto (and Supplier Guarantors) shall pay their respective legal fees and other costs and expenses incurred in connection with the preparation, execution and delivery of this Agreement and all documents and instruments executed pursuant hereto and any other costs and expenses whatsoever and howsoever incurred.

18.3 Benefit of this Agreement

(a) This Agreement shall inure to the benefit of and be binding upon the respective successors and permitted assigns of the Parties hereto (and the Supplier Guarantors).

(b) Except as expressly set forth in the foregoing Sections 18.3(a) or 13.1 or Section 18.12, nothing in this Agreement shall be construed to give any rights or benefits to anyone other than the City, the Supplier and the Supplier Guarantors.

18.4 Entire Agreement

This Agreement constitutes the entire agreement between the Parties hereto (and the Supplier Guarantors) with respect to the subject matter hereof and cancels and supersedes any prior understandings and agreements between the Parties hereto (and the Supplier Guarantors) with respect thereto. There are no representations, warranties, terms, conditions, undertakings or collateral agreements, express, implied or statutory, between the Parties (or the Supplier Guarantors) in relation to the subject matter hereof other than as expressly set forth in this Agreement.

18.5 Amendments and Waiver

Subject to Section 3.11, no modification of or amendment to this Agreement is valid or binding unless set forth in writing and fully executed by both of the Parties hereto (and the Supplier Guarantors) and no waiver of any breach of any term or provision of this Agreement is effective or binding unless made in writing and signed by the Party or Supplier Guarantor purporting to give such waiver and, unless otherwise provided, is limited to the specific breach waiver.

18.6 Notices

(a) Any order, demand, notice or other similar communication to be given to a Party or a Supplier Guarantor in connection with this Agreement must be given in writing and shall be deemed to be validly given if given to the persons named below by personal delivery, registered mail, by courier or by email (provided if the Party sending notice receives an "out of office" or equivalent reply from the receiving Party, the sender must re-send the notice to the person named in such "out of office" reply), or, in each case to such other individual as is designated in writing by the relevant recipient Party or Supplier Guarantor at the relevant address or email listed below:

(i) if to the Supplier:

Zeco Systems (Canada) Inc.
767 S. Alameda St., Suite 200
Los Angeles, California 90021

Attention: John Murnin
Email: jmurnin@greenlots.com

and

Attention: Carita Walker
Email: cwalker@greenlots.com

(ii) If to Zeco Systems:

Zeco Systems, Inc.

767 S. Alameda St., Suite 200
Los Angeles, California 90021

Attention: Carita Walker
Email: cwalker@greenlots.com

(iii) If to Zeco Holdings:

Zeco Holdings, Inc.
767 S. Alameda St., Suite 200
Los Angeles, California 90021

Attention: Carita Walker
Email: cwalker@greenlots.com

(iv) if to the City:

City of Vancouver

453 West 12th Avenue
Vancouver, BC V5Y 1V4

Attention: Lon LaClaire, General Manager, Engineering Services
Email: Lon.laclaire@vancouver.ca

Attention: Francie Connell, Q.C., Director, Legal Services
Email: francie.connell@vancouver.ca

Copied to:

Attention: each City's Manager to their respective email addresses

Attention: David Li, Legal Counsel
Email: david.li@vancouver.ca

or such other address, email or facsimile number as may be designated by notice given by either Party or Supplier Guarantor to the other, provided that, notwithstanding the foregoing, the Supplier's invoices shall be addressed as specified in Section 9.3 or as otherwise specified in the relevant City purchase order.

(b) Any order, demand, notice or other communication given in accordance with Section 18.6(a) shall be conclusively deemed to have been given:

(i) if given by personal delivery, on the day of actual delivery thereof;

(ii) if given by registered mail or courier, on the Business Day following confirmation by the postal service or the courier that the notice has been delivered; and

(iii) if given by email, on the day of transmittal thereof if given during the normal business hours of the recipient and on the Business Day during which such normal business hours next occur if not given during such hours on any day.

Notwithstanding the foregoing, if the Party or Supplier Guarantor giving any demand, notice or other communication knows or ought reasonably to know of any difficulties

with the postal or other system of delivery which might affect the delivery of any such demand, notice or other communication, the Party or Supplier Guarantor must use an alternate method of delivery permitted in this section.

18.7 Governing Law and Jurisdiction

(a) This Agreement is governed by and must be construed in accordance with the laws of the Province of British Columbia.

(b) All provisions of the *International Sale of Goods Act* (British Columbia) are specifically excluded from application to this Agreement.

(c) This Agreement is subject to the exclusive jurisdiction of the courts in the Province of British Columbia except:

(i) as otherwise agreed by the Parties (or the Supplier Guarantors) pursuant to ARTICLE 17; and

(ii) to the extent necessary to enforce, in another jurisdiction, any decision or award made pursuant to ARTICLE 17 or any judgment of any court in the Province of British Columbia.

18.8 Further Assurances

Each Party agrees to do all things and execute all deeds, instruments, transfers or other documents as may be necessary or desirable to give full effect to the provisions of this Agreement and the transactions contemplated by it.

18.9 Severance

If any term or condition of this Agreement is for any reason held to be illegal, invalid, ineffective, inoperable or otherwise unenforceable, it shall be severed and deemed to be deleted from this Agreement and the validity and enforceability of the remainder of this Agreement shall not be affected or impaired thereby. If any term or condition of this Agreement is found to be illegal, invalid ineffective, inoperable or otherwise unenforceable, but would not be so if some part of it were deleted, the term or condition shall apply with such modifications as may be necessary to make it enforceable.

18.10 Counterparts

This Agreement may be executed in any number of counterparts. All counterparts, taken together, constitute one instrument. A Party and the Supplier Guarantors may execute this Agreement by signing any counterpart.

18.11 Independent Legal Advice

THE SUPPLIER ACKNOWLEDGES THAT THE SUPPLIER HAS BEEN GIVEN THE OPPORTUNITY TO SEEK INDEPENDENT LEGAL ADVICE BEFORE EXECUTING THIS AGREEMENT.

18.12 Guarantee by Supplier Guarantors of Supplier's Obligations

(a) Supplier is responsible for performing all its obligations hereunder with respect to the Supply. Supplier Guarantors hereby unconditionally, absolutely and irrevocably guarantee to and in favour of the City to perform and observe all of the agreements, covenants and obligations of the Supplier under this Agreement (collectively, "**Guaranteed Obligations**"). Supplier Guarantors are party to this Agreement solely for

the purpose of guaranteeing of the Guaranteed Obligations as provided in this Section 18.12.

(b) The Parties and Supplier Guarantors acknowledge and agree that: (i) the guarantee set out in Section 18.12(a) shall be a continuing guarantee and covers any and all surviving agreements, covenants and obligations of the Supplier under this Agreement; (ii) no neglect or forbearance of the City in attempting to enforce observance of this Agreement, no extension of time which may be given by the City from time to time to the Supplier, no waiver or other indulgences, and no other act or failure to act in attempting to enforce observance of this Agreement by the City will release, discharge or in any way reduce the obligations of the Supplier Guarantors under this Section 18.12; and (iii) the City shall not be obligated to exhaust its resource against the Supplier before being entitled to performance from Supplier Guarantors.

(c) The obligations of Supplier Guarantors are independent of the obligations of the Supplier and a separate action or actions may be brought and prosecuted against Supplier Guarantors, whether or not actions are brought against the Supplier or whether the Supplier is joined in any such action.

(d) Upon any failure of the Supplier to punctually perform any of the Guaranteed Obligations(inclusive of any applicable cure periods provided herein to Supplier), Supplier Guarantors shall forthwith perform such obligations upon written demand by the City, provided delay by the City in making a demand for performance shall in no event affect Supplier Guarantor's obligations under this Section 18.12. The rights, powers, remedies, and privileges provided in this Section 18.12 are cumulative and not exclusive of any rights, powers, remedies, and privileges provided by any other agreement or by Law.

(e) Provided any cure periods applicable to Supplier under this Agreement have expired and further provided that the City has complied with its notification obligations herein to Supplier, Supplier Guarantors waive presentment, demand, notice of dishonor, protest, nonpayment and all other notices whatsoever, including without limitation: notice of acceptance hereof; notice of all contracts and commitments; notice of the existence or creation of any liabilities under this Agreement and of the amount and terms thereof; and notice of all defaults, disputes or controversies between the City and the Supplier resulting from this Agreement or otherwise, and the settlement, compromise or adjustment thereof.

(f) Notwithstanding anything else contained in this Section 18.12, Supplier Guarantors' obligations with respect to the Guaranteed Obligations are subject, in all respects, to the limitations, exclusions, conditions and remedies provided to Supplier in this Agreement.

18.13 Electronic Execution

Delivery of an executed signature page to this Agreement by either Party or a Supplier Guarantor by electronic transmission shall be as effective as delivery of a manually executed copy of this Agreement by such Party.

IN WITNESS WHEREOF this Agreement has been executed as of the day and year first above written by and on behalf of the Parties and the Supplier Guarantors by their duly authorized signatories.

ZECO SYSTEMS (CANADA) INC.

s.15(1), s.22(1)

Signature

Andreas Lips, CEO
Print Name and Title

CITY OF VANCOUVER

s.15(1), s.22(1)

Signature

George Kavouras, Category Manager
Supply Chain Management
Print Name and Title

s.15(1), s.22(1)

Signature

Alexander Ralph, Chief Procurement Officer
Supply Chain Management
Print Name and Title

s.15(1), s.22(1)

Signature

Lon L L LaClaire, General Manager
Engineering Services
Print Name and Title

s.15(1), s.22(1)

Signature

Francie Connell, Director and City Solicitor
Legal Services
Print Name and Title

ZECO SYSTEMS, INC.

s.15(1), s.22(1)

Signature

Andreas Lips, CEO
Print Name and Title

ZECO HOLDINGS, INC.

s.15(1), s.22(1)

Signature

Andreas Lips, CEO
Print Name and Title

SCHEDULE A -
SCOPE OF GOODS AND SERVICES

General Scope of Goods and Services to be performed by Greenlots:

The Supplier will, in accordance with the terms and conditions of the Agreement, notwithstanding any term below to the contrary, supply all of the goods and services described in this Schedule A and in the Agreement to the City for the prices and compensation set out in Schedule B save and except for any good or service expressly set out in the column below titled "City of Vancouver" that is to be supplied or carried out by the City. Without limiting the generality of the foregoing, the Supplier will supply, deliver, install, test, commission, operate, network, and maintain all EVSE's for the City. The information set out below in the column titled "Greenlots" is not intended to limit or restrict the obligations of the Supplier under this Agreement but is intended to merely provide non-exhaustive examples of obligations to be performed by Greenlots.

Defined Terms:

Each term used in this Schedule A will have the following meaning:

- "EV" means a vehicle that is powered solely by battery or a combination of battery and internal combustion engine.
- "EVSE" means Electric Vehicle Supply Equipment an EV charging station supplied by the Supplier to the City in accordance with the terms of the Agreement. This includes the charger and connected components, cables(s) and charging connector(s).
- "Kiosk" means housing for electrical or electronic equipment. Its purpose is to protect that equipment from the environment (especially in the case of external electrical enclosures), to protect people from the equipment and to distribute electrical power, in this case power to EV stations.
- "Point of Interconnection" means where City electrical infrastructure meets Hydro (within a kiosk).
- "Temporary special zone" means temporary signage, which includes signage relating prohibiting parking during civil and electrical installations of EV infrastructure.
- "Turnkey" means the Supplier is responsible for all tasks in accordance with Section 3.1 of the Agreement.

		RESPONSIBILITY	
#	SPECIFIC FUNCTIONS	GREENLOTS	CITY OF VANCOUVER
1	Site selection	The Supplier will: • Provide industry experience and guidance to optimize site selection as required by the City, on a consulting basis as deemed necessary by Greenlots and the City. Site selection consulting to be billed at Greenlots Project Management hourly rate. • Seek site data from the City to proceed with the design for the site.	The City will: • Determine City sites and provide relevant site data to Greenlots. • Provide sites specification requirements (i.e. number of stations, layout and configuration per site, etc.). • Provide information relating to site conditions (i.e. existing conditions of subsurface and surface, soil conditions if available (case by case basis), existing geotechnical information, property surveys and setback requirements, information on utilities, technical information on existing and future known structures and systems and their constraints on the design, and cellular signal strength and signal quality at each site). • Provide site details including address, site host contact information and any site-specific requirements or guidance and health and safety considerations. • Provide coordination with appropriate site stakeholders, (i.e. site owner, site contacts, neighbors) • Ensure all relevant site-use approvals, site-use agreements and all related site-use terms and conditions. • Provide preferred metering information depending on a site by site basis as requirements may change based on the site

2	**Hardware** **(ordering, supply and delivery)**	The Supplier will supply and deliver all EVSE hardware, which includes charging station equipment, cables, fittings and all other hardware required to ensure all stations are usable by users in the normal course. **EVSE Hardware** The Supplier will: • Engage the City with regards to project needs, including schedule requirements and specific site characteristics. • Make EVSE hardware recommendation based on site requirements as well as their experience and current OEM performance and their understanding of the risks, costs, and benefit trade-offs of OEM products. • Provide the City with a comprehensive quote detailing description of EVSE Hardware, quantities, unit costs including costs for Extended OEM parts-warranties, shipping costs, taxes, lead times and any other information required by the City. The City will make the ultimate decision on the EVSE hardware that is selected. • Place the order as per the Purchase Order and will supply and delivery the required EVSE hardware. • Confirm ability to meet scheduling needs for all EVSE hardware on a site-by-site basis. Estimated lead times are shown in Schedule C. **Load Management Hardware (optional)** The Supplier may: • Help the City reduce both Capex and Opex costs through the Load Management functionality of our SKY Network. Greenlots will accomplish this functionality through software embedded in the charging station, or through a separate site controller provided by Greenlots. • Offer Load Management solution to the City and its value to City will vary site-by-site, based on EVSE product mix, operational objectives, project budget and planned EVSE utilization. • Provide site-by-site recommendations to the City including preliminary solution design, pricing and lead times for its Load Management solution. These recommendations will be informed by the City. • Provide load scheduling which enables the City to prevent or curtail charging sessions during hours when the cost of electricity is high. Based on utility tariffs, site hosts can manually set the maximum site load for specific hours during a day. • Provide load sharing which can enable the City to install more EV chargers than the site's circuit breaker, panel or transformer capacity would otherwise allow. Greenlots SKY EV Charging Network Software uses customizable algorithms that enable customers to set a maximum charging load limit allowing for automatic sharing of available power between EV chargers, when charging load is expected to go beyond its limit.	The City will: • Issue a Purchase Order to Greenlots once the EVSE hardware is selected. • Provide Greenlots information on project needs, including scheduling and specific site characteristics including EVSE hardware specifications (i.e. L2, L3, port count, desired kWh) • Supply all power kiosks required for each project scope • Review all COV supplied hardware shop drawings prior to providing the above information to Greenlots.
3	**Design (Greenlots to tender at City discretion)** (includes all drawings and IFC's, Engineer of Record for all signed and sealed drawings) and Site design (including	The Supplier will: • Select Engineer of Record subcontractor with City review and approval. (Program Level, per Project Management section). • Assess site data provided by City for construction feasibility and site operability. • Schedule and perform site walk. • After site walk, submit a pricing proposal including preliminary layouts, exclusions and assumptions. • Upon approval of the preliminary site layout by City, develop site-engineering plan. • Produce the final IFR engineering drawings and invite City to participate in review. • Act as engineer of record (Greenlots or designated sub-contractor). • Provide sealed engineering drawings for sites as required by local electrical safety and construction standards.	The City will: • Provide authorization to proceed when final IFC drawings are issued. • Share any design specifications with Greenlots.

	civil and electrical)		
4	**Electrical metering, connection and service**	The Supplier will:Provide sub-metering for all new connections for BC Hydro provisions and existing City electrical services, and retrofit existing infrastructure with sub-meters as necessary. • Coordinate and work with BC Hydro to have each EVSE connected and serviced with electricity. • Coordinate and work with BC Hydro for interconnection and service upgrades as required.	The City will: • Be the lead applicant to BC Hydro for all new electrical service(s).
5	**Installation (Greenlots to tender at City discretion)**	The Supplier will: • Lead, manage, install, and report on infrastructure installations. • Provide the City with a primary Project point of contact. • Assume responsibility from the Point of Interconnection (POI) or the connection with the existing building electrical infrastructure. • Install balance of plant materials, including make-ready materials (i.e. transformers, protection equipment, kiosks), as well as all cables, connectors and interfaces for full operation. • Construct and install EV charging station from the POI to the EVSE. • Complete all civil works (e.g. trenching, restoration, concrete pads etc.). • Hire and manage any subcontractors as required. • Apply for construction permits as needed (i.e. electrical, drilling, lane, or road closure permits) and associated traffic management plans. • Ensure all electrical works adhere to code and electrical safety standards. • Arc Flash test as required by BC Hydro. • Develop, complete and adhere to all Site Safety Plans. • Complete project management and project progress reporting as required. • Schedule electrical inspections, trench and final. • Submit As-built drawings. • Provide and complete On-site commissioning support. Provide and complete remote commissioning support. • Provide and complete closeout and turnover documentation. • Complete concrete curb, asphalt and paint job repairs as needed. • Complete site clean-up and restoration. Landscape restorations will vary from site to site as noted in the exclusions. • Provide the best pricing for each City site and the City program in total. To achieve greatest cost efficiencies, subcontractors will be competitively procured through Greenlots' Contracts & Procurement team.	The City will: • Provide guidance on traffic management plans and development permits as required. • Complete new surveys such as environmental, archaeological, land, soils and geotechnical studies. • Mitigate unforeseen and/or less than ideal subsurface or soils conditions. • Be responsible for utility Interconnection scopes & Fees. • Provide special permits such as building permits and sign permits, if required. • Be responsible for land easements or right-of-way agreements with 3rd parties. • Provide lighting solutions if required. • Provide resources when special or temporary signage is required. • Use City resources as and when required.
6	**Project Management**	The Supplier will: • Work closely with the City to define a project scope which will include Civil, Electrical and Installation requirements on a project-by-project basis. • Work with the City to establish a list of qualified, local subcontractors capable of delivering the defined project scope. • Issue a Request for Proposal to the list of prequalified subcontractors and manage the entire competitive bidding process including bid evaluations, subcontractor selection, negotiations and contracting for the required project scope. • Work with selected subcontractors engineer of record who will be familiar with City and BC Hydro standards, to design the best-fit EV charging infrastructure for the CoV needs. • After site selection, Greenlots will manage site design, as well as subcontractors and installation partners, obtain all required permitting, coordinate with BC Hydro, oversee construction management by subcontractors, and ensure the charging units are fully functional once installed.	The City will: • Review Project progress and escalate issues within the City as and when required through the City's designated contract manager.

		• Add a 15% mark-up on the subcontractors invoice for Program Management.	
7	Station Branding	The Supplier will: • Project manage and implement agreed upon CoV branding for its charging infrastructure. This includes implementation, quality control and assurance. • Select wrapping services subcontractor with City review and approval. (Program Level, per Project Management section). • Coordinate the wrapping of equipment once a design is approved and received by the City. • Provide layout requirements in accordance with EVSE manufacturer requirements.	The City will • Design and develop images for EVSE per City communications guidelines. • Lead initiatives with respect to branding / infographics. • Approve designs and branding of all EVSE's.
8	Utility costs	The Supplier will: • Apply on the City's behalf and work/coordinate with BC Hydro to complete service connection.	The City will: • Pay BC Hydro costs directly. • Hold holds utility accounts and pay utility bills
9	BC Hydro projects	The Supplier will: • Not be subject to BC Hydro-led projects and initiatives, such as BC Hydro owned DCFC on City lands.	The City will: • Lead and manage all BC Hydro related projects including obtaining BC Hydro design approvals for electrical services and coordinating new service connections. • Liaise with BC Hydro on any outage or damage related issues.
10	Contract Manageme nt	The Supplier will: • Ensure compliance with Agreement.	The City will: • Provide MSA contract management and oversight, including regular meetings with Greenlots and enforce performance management. • Organize monthly meetings between the relevant designated City and Greenlots representatives to discuss projects, issues, performance, challenges, deployment schedules and compliance against metrics.
11	Reporting	The Supplier will: • Thru SKY/Insights, provide the City access to reports , including but not limited to the following metrics: o Resolution times(via SKY/Insights) o Up Time (uptime % by station via SKY/Insights). o Usage Utilization (by site via SKY/Insights). o Station availability (measure of % of time when one station at a site is unoccupied via SKY/Insights). o Charging to idle ratio (by site or station) via SKY/Insights. o Energy consumption (by site) via SKY/Insights. o Station downtime (by site and station) (e.g., damage, breaker fault, network issue, etc.). via SKY/Insights o Revenue via SKY/Insights. o Peak demand (by site) via SKY/Insights. Subject to Section 8.1(a), the Supplier will provide a monthly report providing the following data: o Date, start and end time of each charging session o Unique identifier (reference#) of each transaction, or some other way to identify a specific charge session at a specific EV station o Charging rate paid by drivers o Charging fees collected by GL	

		○ GST (driver paid) collected by GL A sample of the monthly report is shown in Schedule A - Appendix 1 (Format of Report required by 8.1(a) and 8.1(b).	
12	**Other external interfaces**	The Supplier will: • Complete all electrical and building permitting and inspection. • Provide and install all temporary special zone permits as required. • Coordinate soil remediation as needed. • Develop and implement traffic management plans, coordinating with the City as required. • Coordinate with the City all necessary street lighting as required. • Complete pre-work hazard identification, including underground utility location • Coordinate with the City's Parks Arborists as required • Coordinate with the City on permanent signage as required • Liaise with the City on routine activities such as permit applications (including electrical, development, street / lane closure, etc.) by following regular public City processes.	The City will: • Lead and act as the triage point between all coordination efforts between City departments and Greenlots except where it would create a process conflict with public City processes such as permit applications. The Agreement does not influence or bind City departments acting in their regulatory capacity. This includes: • Designated City staff acting as the first point of contact between Greenlots and the City, for all non-routine activities. • Development of new programs that would involve the deployment of public charging infrastructure led by other City departments who will consult with the City's Engineering team prior to engaging Greenlots.

SCHEDULE A - APPENDIX 1
FORMAT OF REPORT REQUIRED BY 8.1(A) AND 8.1(B)

SAMPLE GREENLOTS MONTHLY REMITTANCE REPORT

Network :
Enterprise :
Start Period :
End Period :
Report Date :
Time Zone:

S.N.	Device Group	Location	Start Time	End Time	Station ID	Energy (kWh)	Duration	Sale Amount	Tax1 Detail	Tax1	Tax2 Detail	Tax2	Others Tax Detail	Other Tax	Payment Details	Payment Fee	Level Fee	Net	Discount Amount	Payment Gateway	Subscription

SCHEDULE B -
PRICES FOR SUPPLY

Excel file with seven (7) tabs

Note: the Excel file is provided as an attachment in this electronic executed PDF copy of the Agreement.

Work Result Type	Unit of Measure	5-year Fixed Price	Comments
EVSE			
L2			
ABB 32A AC wallbox single port (Shell Recharge Branded) *availability est. Q4 but OEM uncertain*			
Equipment	per station	$ 1,525	ABB 32A Smart Charger L2, single port, HMI screen, 4G, Double Ethernet, 25ft SAE J1772 cable, 2 yr parts warranty, RFID, remote commissioning support (see specs for all features)
Pedestal	per station	$ 755	Indicative price subjet to change. Pedestal is in production, cost is an estimate and may vary
Shipping	per station	$ 200	Cost to deliver physical charging station to the City of Vancouver installation site, GL installation subcontractor or storage. [one time shipping fee regardless of initial destination
Extended Parts Warranty (for total of 5 years)	per station	$ 400	Indicative price subject to change. New product. OEM warranty is 2 years, this cost covers 3 additional years for a total of 5 years. Parts only.
ABB 32A AC wallbox not yet field ready and tested; not available until Q3 2021			
BTC Pedestal Single Port 30A			
Equipment	per station	$ 5,304	Includes BTC single port L2, cord retractors, cell modem, 2 yr parts warranty, RFID, remote commissioning support (see specs for all features)
Shipping	per station	$ 182	Cost to deliver physical charging station to the City of Vancouver installation site, GL installation subcontractor or storage. [one time shipping fee regardless of initial destination
Extended Parts Warranty (for total of 5 years)	per station	$ 360	OEM warranty is 2 years, this cost covers 3 additional years for a total of 5 years. Parts only.
Extended Parts Warranty is not required if CofV chooses O&M Option C Greenlots Care Plan			
BTC Pedestal Dual Port 30A			
Equipment	per station	$ 6,864	Includes BTC dual single port L2, EVSE, cord retractors, cell modem, 2 yr parts warranty, RFID, remote commissioning support (see specs for all features)
Shipping	per station	$ 182	Cost to deliver physical charging station to the City of Vancouver installation site, GL installation subcontractor or storage. [one time shipping fee regardless of initial destination
Extended Parts Warranty (for total of 5 years)	per station	$ 420	OEM warranty is 2 years, this cost covers 3 additional years for a total of 5 years. Parts only.
Extended Parts Warranty is not required if CofV chooses O&M Option C Greenlots Care Plan			
EV Box Businessline Single port (Hub option - first station must be a Hub) *10-12 wk delivery*			
Equipment	per station	$ 2,658	Single port, hub with modem, 18ft cable with RFID, white (see specs for all features)
Equipment	per station	$ 2,833	Single port, hub with modem, 25ft cable with RFID, white (see specs for all features)
Cable retractor and pole	per station	$ 774	Pole mount pedestal and cable retractor
Shipping	per station	$ 182	Cost to deliver physical charging station to the City of Vancouver installation site, GL installation subcontractor or storage. [one time shipping fee regardless of initial destination
Extended Parts Warranty (for total of 5 years)	per station	$ 175	OEM warranty is 3 years, this cost covers 2 additional years for a total of 5 years. Parts only.
Extended Parts Warranty is not required if CofV chooses O&M Option C Greenlots Care Plan			
EV Box Businessline Single port (Satellite option - hardwired to the Hub) *10-12 wk delivery*			
Equipment	per station	$ 2,558	Single port, satellite hardwired to hub, 18ft cable with RFID, white (see specs for all features)
Equipment	per station	$ 2,733	Single port, satellite hardwired to hub, 25ft cable with RFID, white (see specs for all features)
Cable retractor and pole	per station	$ 774	Pole mount pedestal and cable retractor
Shipping	per station	$ 182	Cost to deliver physical charging station to the City of Vancouver installation site, GL installation subcontractor or storage. [one time shipping fee regardless of initial destination
Extended Parts Warranty (for total of 5 years)	per station	$ 175	OEM warranty is 3 years, this cost covers 2 additional years for a total of 5 years. Parts only.
Extended Parts Warranty is not required if CofV chooses O&M Option C Greenlots Care Plan			
EV Box Businessline Double port (Hub option - first station must be a Hub) *10-12 wk delivery*			
Equipment	per dual port station	$ 5,256	Dual port, hub with modem, 18ft cable with RFID, white (see specs for all features)
Equipment	per dual port station	$ 5,606	Dual port, hub with modem, 25ft cable with RFID, white (see specs for all features)
(2) Cable retractor and pole	per dual port station	$ 1,123	Pole mount pedestal and (2) cable retractor
Shipping	per dual port station	$ 350	Cost to deliver physical charging station to the City of Vancouver installation site, GL installation subcontractor or storage. [one time shipping fee regardless of initial destination
Extended Parts Warranty (for total of 5 years)	per dual port station	$ 250	OEM warranty is 3 years, this cost covers 2 additional years for a total of 5 years. Parts only.
Extended Parts Warranty is not applicable if CofV chooses O&M Option C Greenlots Care Plan			
EV Box Businessline Double port (Satellite option - hardwired to the Hub) *10-12 wk delivery*			
Equipment	per dual port station	$ 5,056	Dual port, satellite hardwired to hub, 18ft cable with RFID, white (see specs for all features)
Equipment	per dual port station	$ 5,406	Dual port, satellite hardwired to hub, 25ft cable with RFID, white (see specs for all features)
(2) Cable retractor and pole	per dual port station	$ 1,123	Pole mount pedestal and (2) cable retractor
Shipping	per dual port station	$ 350	Cost to deliver physical charging station to the City of Vancouver installation site, GL installation subcontractor or storage. [one time shipping fee regardless of initial destination
Extended Parts Warranty (for total of 5 years)	per dual port station	$ 250	OEM warranty is 3 years, this cost covers 2 additional years for a total of 5 years. Parts only.
Extended Parts Warranty is not applicable if CofV chooses O&M Option C Greenlots Care Plan			
DCFC			
Tritium RT50 50kW DCFC			
Equipment	per station	$ 31,086	Veefil RT 50kW; dual port, includes EVSE, 12 ft cables, cell modem, 3 yr parts warranty, RFID, remote commissioning (No cable management avaialble on this SKU) (see specs for all features)
Shipping	per station	$ 995	Cost to deliver physical charging station to the City of Vancouver installation site, GL installation subcontractor or storage. [one time shipping fee regardless of initial destination
Extended Parts Warranty (for total of 5 years)	per station	$ 2,733	OEM parts warranty is 2 years; this cost covers 3 additional warranty years for a total of 5 years. Parts only.
Extended Parts Warranty is not required if CofV chooses O&M Option C Greenlots Care Plan;			
Tritium RTM50 50kW DCFC - Better			
Equipment	per station	$ 40,128	RTM50 50kW; (BETTER) dual port CCS/CHAdeMO, includes EVSE, 20 ft cables, cell modem, cable management, 2 yr parts warranty, RFID, remote commissioning (see specs for all features)
Shipping	per station	$ 995	Cost to deliver physical charging station to the City of Vancouver installation site, GL installation subcontractor or storage. [one time shipping fee regardless of initial destination
Custom EVSE branding - production application	per station	$ 675	$675 for initial production and application; $400 for additional sets or re-wrapping
Extended Parts Warranty (for total of 5 years)	per station	$ 8,427	OEM parts warranty is 2 years; this cost covers 3 additional warranty years for a total of 5 years. Parts only.
Extended Parts Warranty is not required if CofV chooses O&M Option C Greenlots Care Plan;			
Due to this being a new SKU, O&M pricing below for Option B & C does not apply; would need to be priced			
Tritium RTM50 50kW DCFC - Best			
Equipment	per station	$ 48,068	RTM50 50kW; (BEST) dual port CCS/CHAdeMO, includes EVSE, 20 ft cables, cell modem, cable management, 2 yr parts warranty, RFID, remote commissioning, custom graphics (see specs for all features)
Shipping	per station	$ 995	Cost to deliver physical charging station to the City of Vancouver installation site, GL installation subcontractor or storage. [one time shipping fee regardless of initial destination
Custom EVSE branding - production application	per station	$ -	Included in unit price
Extended Parts Warranty (for total of 5 years)	per station	$ 10,094	OEM parts warranty is 2 years; this cost covers 3 additional warranty years for a total of 5 years. Parts only.
Extended Parts Warranty is not required if CofV chooses O&M Option C Greenlots Care Plan;			
Due to this being a new SKU, O&M pricing below for Option B & C does not apply; would need to be priced			
Tritium RTM75 75kW DCFC - Better			
Equipment	per station	$ 48,757	RTM75 75kW; (BETTER) dual port CCS/CHAdeMO, includes EVSE, 20 ft cables, cell modem, cable management, 2 yr parts warranty, RFID, remote commissioning (see specs for all features)
Shipping	per station	$ 995	Cost to deliver physical charging station to the City of Vancouver installation site, GL installation subcontractor or storage. [one time shipping fee regardless of initial destination
Custom EVSE branding - production application	per station	$ 675	$675 for initial production and application; $400 for additional sets or re-wrapping
Extended Parts Warranty (for total of 5 years)	per station	$ 10,239	OEM parts warranty is 2 years; this cost covers 3 additional warranty years for a total of 5 years. Parts only.
Extended Parts Warranty is not required if CofV chooses O&M Option C Greenlots Care Plan;			
Due to this being a new SKU, O&M pricing below for Option B & C does not apply; would need to be priced			
Tritium RTM75 75kW DCFC - Best			
Equipment	per station	$ 56,698	RTM75 75kW; (BEST) dual port CCS/CHAdeMO, includes EVSE, 20 ft cables, cell modem, cable management, 2 yr parts warranty, RFID, remote commissioning, custom graphics (see specs for all features)
Shipping	per station	$ 995	Cost to deliver physical charging station to the City of Vancouver installation site, GL installation subcontractor or storage. [one time shipping fee regardless of initial destination
Custom EVSE branding - production application	per station	$ -	Included in unit price
Extended Parts Warranty (for total of 5 years)	per station	$ 11,906	OEM parts warranty is 2 years; this cost covers 3 additional warranty years for a total of 5 years. Parts only.
Extended Parts Warranty is not required if CofV chooses O&M Option C Greenlots Care Plan;			
Due to this being a new SKU, O&M pricing below for Option B & C does not apply; would need to be priced			
ABB Terra 54 50kW DCFC (Shell Recharge Branded)			
Equipment	per station	$ 34,719	Terra 54 (ULT54C)) - 50 kW DCFC dual port, 20 ft CCS-1 Cables, RFID Reader, LED Display, cellular modem, 2 year warranty (see specs for all features) NOTE: this is not the HV version
Equipment	per station	$ 37,488	Terra 54 (ULT54CJ)) - 50 kW DCFC dual port, 20 ft CCS-1 and Chademo Cables, RFID Reader, LED Display, cellular modem, 2 year warranty (see specs for all features) NOTE: this is not the HV version
Cable Management	per station	$ 2,760	Terra 54 Cable Management System (2) connectors - optional
Shipping	per station	$ 1,184	Cost to deliver physical charging station to the City of Vancouver installation site, GL installation subcontractor or storage. [one time shipping fee regardless of initial destination
Extended Parts Warranty (for total of 5 years)	per station	$ 5,070	OEM warranty is 2 years, this cost covers 3 additional years for a total of 5 years. Parts only.
Extended Parts Warranty is not required if CofV chooses O&M Option C Greenlots Care Plan			
BTC Slim 50kW DCFC			
Equipment	per station	$ 32,753	50kW Slim 480VAC CHAdeMO/CCS1; 20 ft cables; 15" High-Resolution Color Touchscreen LCD, Cellular Modem, RFID Reader, Cord Retraction, including cable management (see specs for all features)
Equipment	per station	$ 41,123	50kW Slim 208VAC CHAdeMO/CCS1; 20 ft cables, 15" High-Resolution Color Touchscreen LCD, Cellular Modem, RFID Reader, Cord Retraction (see specs for all features)
Shipping	per station	$ 995	Cost to deliver physical charging station to the City of Vancouver installation site, GL installation subcontractor or storage. [one time shipping fee regardless of initial destination
Extended Parts Warranty (for total of 5 years)	per station	$ 3,740	OEM warranty is 2 years, this cost covers 3 additional years for a total of 5 years. Parts only.

Due to reliability and service concerns, the BTC Slim 50kW DCFC not available under O&M Option C Greenlots Care. This may change in 2021 and Greenlots will keep the City posted of developments					
Load Management Hardware - optional					
Load Management and Communications Solution		per site	$ 13,300	Site controller, Revenue Meter, CTs, switch, modem, enclosure, design, hw installation, sw commissioning (see specs for all features)	
	Includes Greenlots Site Controller, meter, CTs	per site		Load Management hardware, if the site requirements and overall use-case make sense	
	Includes switch, modem, enclosure	per site		Communications hardware	
Shipping		per site	$ 250	Cost to ship all load management and communications hardware to City of Vancouver installation site, installation subcontractor or storage [one time shipping fee regardless of initial destination]	
Network Operating Software Subscription Fees					
L2					
All Single Port L2s					
SKY Network Management Platform		per single port station per year	$ 530	Annual subscription price	
	SKY Administrative Platform	Included in subscription			
	Driver Portal	Included in subscription			
	Mobile Application	Included in subscription			
	Tier 1 & Tier 2 Customer Support	Included in subscription			
	Cellular Data Fees	Included in subscription			
Load Mangement Software module		per single port station per year	$ 125	If Load Management solution is installed - optional	
EV Charging Transaction Fee		Per paid charging transaction	10%	See Schedule G; Greenlots reimburses CoV for all Revenue transactions monthly and retains 10% of all Revenue as collection and processing fee.	
All Dual Port L2s		per dual port station per year			
SKY Network Management Platform		per dual port station per year	$ 1,060	Annual subscription price	
	SKY Administrative Platform	Included in subscription			
	Driver Portal	Included in subscription			
	Mobile Application	Included in subscription			
	Tier 1 & Tier 2 Customer Support	Included in subscription			
	Cellular Data Fees	Included in subscription			
Load Mangement Software module		per dual port station per year	$ 125	If Load Management solution is installed - optional	
EV Charging Transaction Fee		Per paid charging transaction	10%	See Schedule G; Greenlots reimburses CoV for all Revenue transactions monthly and retains 10% of all Revenue as collection and processing fee.	
DCFC					
All DCFCs					
SKY Network Management Platform		per DCFC per year	$ 795	Annual subscription price	
	SKY Administrative Platform	Included in subscription			
	Driver Portal	Included in subscription			
	Mobile Application	Included in subscription			
	Tier 1 & Tier 2 Customer Support	Included in subscription			
	Cellular Data Fees	Included in subscription			
Load Mangement Software module		per DCFC per year	$ 125	If Load Management solution is installed - optional	
EV Charging Transaction Fee		Per paid charging transaction	10%	See Schedule G; Greenlots reimburses CoV for all Revenue transactions monthly and retains 10% of all Revenue as collection and processing fee.	
Operations & Maintenance					
L2					
All Single Port L2s					
O&M Option A (As Needed Plan)				**Option A (T&M O&M) does not include 95% uptime guarantee or 14/21 day resolution guarantee**	
Preventative Maintenance - scheduled		per single port L2 station per visit	$ 140	See Schedule H	
Corrective Maintenance - as needed		per hour	$ 210	See Schedule H	
O&M Option B (Subscription Plan - labor only)				**Option B includes 95% uptime guarantee; does not include 14/21 day resolution guarantee**	
Annual Preventative + Corrective Maintenance per Schedule H		per single port L2 station	$ 3,821	See Schedule H; price is representative of a 5 year term from point of program initiation; price includes labor only and does not include 14/21 day resolution guarantee; Option B requires 5 years parts warranty to be purchased, priced per SKU above	
Biannual Preventative + Corrective Maintenance per Schedule H		per single port L2 station	$ 5,518	See Schedule H; price is representative of a 5 year term from point of program initiation; price includes labor only and does not include 14/21 day resolution guarantee; Option B requires 5 years parts warranty to be purchased, priced per SKU above	
O&M Option C (Greenlots Cares Subscription Plan - parts and labor included)				**Option C includes 95% uptime guarantee and 14/21 day resolution guarantee**	
OEM Parts Warranty 5 years, Annual Preventative + Corrective Maintenance per Schedule H		per single port L2 station	$ 4,035	See Schedule H; price is representative of a 5 year term from point of program initiation; price includes 5 years of Annual Preventative Maintenacne, plus Corrective Maintenance, and parts coverage as described in SCHEDULE H O&M AGREEMENT. Includes 14 day L2 and 21 day DCFC resolution guarantee.	
All Dual Port L2s					
O&M Option A (As Needed Plan)				**Option A (T&M O&M) does not include 95% uptime guarantee or 14/21 day resolution guarantee**	
Preventative Maintenance - scheduled		per dual port L2 station per visit	$ 140	See Schedule H	
Corrective Maintenance - as needed		per hour	$ 210	See Schedule H	
O&M Option B (Subscription Plan - labor only)				**Option B includes 95% uptime guarantee; does not include 14/21 day resolution guarantee**	
Annual Preventative + Corrective Maintenance scheduled + Corrective Maintenance per Schedule H		per dual port L2 station	$ 4,527	See Schedule H; price is representative of a 5 year term from point of program initiation; price includes labor only and does not include 14/21 day resolution guarantee; Option B requires 5 years parts warranty to be purchased, priced per SKU above	
Biannual Preventative Maintenance scheduled + Corrective Maintenance per Schedule H		per dual port L2 station	$ 6,897	See Schedule H; price is representative of a 5 year term from point of program initiation; price includes labor only and does not include 14/21 day resolution guarantee; Option B requires 5 years parts warranty to be purchased, priced per SKU above	
O&M Option C (Greenlots Cares Subscription Plan - parts and labor included)				**Option C includes 95% uptime guarantee and 14/21 day resolution guarantee**	
OEM Parts Warranty 5 years, Annual Preventative + Corrective Maintenance per Schedule H		per dual port L2 station	$ 4,919	See Schedule H; price is representative of a 5 year term from point of program initiation; price includes 5 years of Annual Preventative Maintenance, plus Corrective Maintenance, and parts coverage as described in SCHEDULE H O&M AGREEMENT. Includes 14 day L2 and 21 day DCFC resolution guarantee.	
DCFC					
All DCFCs					
O&M Option A (As Needed Plan)				**Option A (T&M O&M) does not include 95% uptime guarantee or 14/21 day resolution guarantee**	
Preventative Maintenance - scheduled		per DCFC station per visit	$ 280	See Schedule H	
Corrective Maintenance - ad hoc		per hour	$ 210	See Schedule H	
O&M Option B (Subscription Plan - labor only)				**Option B includes 95% uptime guarantee; does not include 14/21 day resolution guarantee**	
Annual Preventative + Corrective Maintenance per Schedule H		per DCFC station	$ 6,669	See Scheudle H; price is representative of a 5 year term from point of program initiation; price includes labor only and does not include 14/21 day resolution guarantee; Option B requires 5 years parts warranty to be purchased, priced per SKU above	
Biannual Preventative + Corrective Maintenance per Schedule H		per DCFC station	$ 8,945	See Schedule H; price is representative of a 5 year term from point of program initiation; price includes labor only and does not include 14/21 day resolution guarantee; Option B requires 5 years parts warranty to be purchased, priced per SKU above	
O&M Option C (Greenlots Cares Subscription Plan - parts and labor included)				**Option C includes 95% uptime guarantee and 14/21 day resolution guarantee**	
Tritium Parts Warranty 5 years, Annual Preventative + Corrective Maintenance per Schedule H		per DCFC station	$ 15,585	See Schedule H; price is representative of a 5 year term from point of program initiation; price includes 5 years of Annual Preventative Maintenane, plus Corrective Maintenance, and parts coverage as described in SCHEDULE H O&M AGREEMENT. Includes 14 day L2 and 21 day DCFC resolution guarantee.	
ABB Parts Warranty 5 years, Annual Preventative + Corrective Maintenance per Schedule H		per DCFC station	$ 13,122	See Schedule H; price is representative of a 5 year term from point of program initiation; price includes 5 years of Annual Preventative Maintenane, plus Corrective Maintenance, and parts coverage as described in SCHEDULE H O&M AGREEMENT. Includes 14 day L2 and 21 day DCFC resolution guarantee.	
On-site diagnostic test charge for all DCFC CM service calls		per DCFC station	$ 315	See Schedule H; $315 is the 5 year price if CofV requires on-site diagnostic test-charge for all DCFC Corrective Maintenance service calls	
Administrative Services					
Program Management		per site or per project	15%	See Scheudle A	
Customized Program / Software Development		per hour	$225		

Work Result Type	Unit of Measure	Estimated Price		Comments
Electrical Design Services				
Electrical Design Services	per hour	$	210.00	Greenlots to contract EoR, separate from construction contractor, price is only estimate for budgeting purposes
EVSE Instalaition				
Soft Landscape				
L2				
1 Station	per station	$	7,212.37	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
2 Stations	per station	$	7,212.37	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
3 Stations	per station	$	7,212.37	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
DCFC				
1 Station	per station	$	9,500.45	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
2 Stations	per station	$	9,500.45	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
Asphalt				
L2				
1 Station	per station	$	7,618.82	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
2 Stations	per station	$	7,618.82	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
3 Stations	per station	$	7,618.82	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
DCFC				
1 Station	per station	$	9,937.09	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
2 Stations	per station	$	9,937.09	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
Concrete				
L2				
1 Station	per station	$	7,843.07	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
2 Stations	per station	$	7,843.07	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)

3 Stations	per station	$	7,843.07	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
DCFC				
1 Station	per station	$	10,190.09	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
2 Stations	per station	$	10,190.09	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
Surface Mount				
L2				
1 Station	per station	$	1,759.89	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
2 Stations	per station	$	1,759.89	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
3 Stations	per station	$	1,759.89	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
DCFC				
1 Station	per station	$	3,482.79	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
2 Stations	per station	$	3,482.79	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
Kiosk Instalaition				
Soft Landscape				
Kisok installation for (1) DCFC or L2	per Kiosk	$	9,244.84	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
Kiosk instalation for up to (3) DCFC	per Kiosk	$	10,656.34	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
Asphalt				
Kisok installation for (1) DCFC or L2	per Kiosk	$	9,651.65	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
Kiosk instalation for up to (3) DCFC	per Kiosk	$	11,184.98	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
Concrete				
Kisok installation for (1) DCFC or L2	per Kiosk	$	9,881.29	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
Kiosk instalation for up to (3) DCFC	per Kiosk	$	11,272.31	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
Surface Mount				
Kisok installation for (1) DCFC or L2	per Kiosk	$	2,243.21	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
Kiosk instalation for up to (3) DCFC	per Kiosk	$	3,411.03	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
Construction (Electrical / Civil / Trenching)				
Soft Landscape				
BC Hydro Service				
(1) x 100mm Duct	per linear foot	$	372.49	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
Pilaster	per pilaster	$	4,938.30	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
L2 - on street				
1 Station	per linear foot	$	351.53	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
2 Stations	per linear foot	$	381.27	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
3 Stations	per linear foot	$	410.99	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
L2 - off street				
1 Station	per linear foot	$	210.92	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
2 Stations	per linear foot	$	228.76	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
3 Stations	per linear foot	$	246.59	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
DCFC - on street				
1 Station	per linear foot	$	366.60	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
2 Stations	per linear foot	$	407.60	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
DCFC - off street				
1 Station	per linear foot	$	219.96	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
2 Stations	per linear foot	$	244.56	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
Asphalt				
BC Hydro Service				
(1) x 100mm Duct	per linear foot	$	603.59	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
Pilaster	per pilaster	$	5,378.94	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
L2 - on street				
1 Station	per linear foot	$	582.63	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
2 Stations	per linear foot	$	612.37	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
3 Stations	per linear foot	$	642.09	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
L2 - off street				
1 Station	per linear foot	$	349.58	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
2 Stations	per linear foot	$	367.42	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
3 Stations	per linear foot	$	385.26	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
DCFC - on street				
1 Station	per linear foot	$	597.70	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
2 Stations	per linear foot	$	638.71	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
DCFC - off street				
1 Station	per linear foot	$	358.62	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
2 Stations	per linear foot	$	383.22	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
Concrete				
BC Hydro Service				
(1) x 100mm Duct	per linear foot	$	678.47	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
Pilaster	per pilaster	$	5,759.33	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
L2 - on street				
1 Station	per linear foot	$	657.51	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
2 Stations	per linear foot	$	687.25	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
3 Stations	per linear foot	$	716.98	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
L2 - off street				
1 Station	per linear foot	$	394.51	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
2 Stations	per linear foot	$	412.35	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
3 Stations	per linear foot	$	430.19	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
DCFC - on street				
1 Station	per linear foot	$	672.58	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
2 Stations	per linear foot	$	713.59	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
DCFC - off street				
1 Station	per linear foot	$	403.55	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
2 Stations	per linear foot	$	428.15	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
Surface Mount				
L2 - on street				
1 Station	per linear foot	$	110.23	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
2 Stations	per linear foot	$	148.88	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
3 Stations	per linear foot	$	187.04	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
DCFC - on street				
1 Station	per linear foot	$	134.70	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
2 Stations	per linear foot	$	194.31	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
Professional Services				
Project Management (or site seleiction consulting services per Schedule A)	per hour	$	200.00	Greenlots to self-perform or contract, price is only estimate for budgeting purposes
Permitting Fees - DCFCs	per site	$	6,500.00	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
Permitting Fees -L2s	per site	$	5,000.00	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
EVSE Branding Services				
L2 - design support	per hour	$	110.00	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
DCFC - design support	per hour	$	110.00	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)

L2 - support (general branding services)	per hour	$	140.00	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
DCFC - support (general branding services)	per hour	$	140.00	Greenlots to tender, price is only estimate for budgeting purposes (estimated pricing assumes the qualifications as outlined in the tabs below)
Load Management Installation [Optional]				
Load Management Installation [Optional]	per site	NA - subject to tender		Optional - work with COV for assessment; Greenlots to tender

POWERPROS
ELECTRICAL

greenlots
A Member of the Shell Group

Date: Oct 14, 2020

Greenlots with Power Pros, is pleased to submit a proposal to provide all labor, supervision, and materials to complete the electrical installation as outlined below and in accordance with the requirements of the 2018 Edition of the Canadian Electrical Code, and its amendments.

The pricing for the below scope of work is provided in attached spreadsheet and is for new installations which require both conduit trenching with a minimum of 10M, one kiosk, and at least one DCFC or L2.

We offer the choice of a fixed 5-year pricing or per year pricing with each year for a 5-year term. These are based off historical construction price increases.

All Pricing includes the following scope and assumptions:

- Construction start time assumed to be scheduled at least 60 days from time of all IFC drawings provided to Power Pros. This excludes projects where a building permit is required as this will require more time.
- Traffic management plan for city approval
- Construction Schedule
- Daily construction progress updates
- Coordination with City and local business/residential of construction requirements
- BC One Call and Shaw Utility call, city utility review
- Utility scan and locate
- First Aid Level 1 on site
- COR certified safety documentation and program
- Construction Management
- Pre-job site meeting
- Construction site setup and tear down
- Garbage bin and removal
- Job Site Fencing
- All precast pads to include concrete (32Mpa, C2 exposure concrete mix design (max.3/4" aggregate, 2 ½" slump, and 5-8% air), reinforced with 2 layers of 15M grid spaced at 12" on center each way, and chamfered edge
- Sawcut and removal of any asphalt or concrete surface
- Excavation (assumed accessible with dump truck for hot load and loadout)
- Assumed available area adjacent to trench to stockpile material for re-use
- Assumed machine moved to excavate
- Removal and dumping of excess soil from site

- Supply and replacement of backfill (as per specs below)
- Tamping
- Compaction testing under asphalt
- Ground prep for precast pads and finished surface (as per specs below)
- Replacement of surface to match existing (as per specs below)
- Duct seal for all underground conduits
- Drain fittings for underground conduits
- Pickup and delivery of all equipment to site
- Concrete mounting hardware supply and install for all equipment
- Concrete sealant applied to all equipment
- Wire pull and terminations
- Coordination with Inspector
- Building shutdown coordination when required
- BC Hydro coordination when required
    - Civil inspector
    - Line crew connection
    - Meter install
- Commissioning of charger/s and kiosk, including test with EV
- Red-line drawings
- Maintenance manual package

Trenching specific scope/specs:

- All pricing based off 10m minimum trench of either surface
- Power for each piece of equipment to be run in dedicated conduit
- **BC Hydro Utility Feed** to allow for (1) 4" DBII duct run to 1M from any underground connection point or pole as per Hydro standards
- **BC Hydro Pilaster** (this is needed when running to a pole) to allow for concrete forming and pouring around conduit and inside pilaster, Excavation of 1M from pole, and a pole hold as per Hydro standards
- **DCFC power feeds** to allow for dedicated conduits to each unit, 3" RPVC conduit underground and 2' EMT with dry type fittings for surface mount installations
- **DCFC Power feed** to be run with (3) #3CU RW90 and (1) #6 RW90 Ground
- **L2 power feeds** to allow for dedicated conduits to each unit, 1 ¼" RPVC conduit underground and 1" EMT with dry type fittings for surface mount installations
- **L2 power feeds** to be run with (2) #8 RW90 and (1) #10 RW90 Ground
- All existing concrete and asphalt surfaces to be max 4" depth
- Replacement of concrete and asphalt to match trench width (additional costs will apply if any areas require replacement of full sidewalk sections)
- **Off-Street trenching** refers job sites which are located on private property and are a minimum of 15M from a city sidewalk, city roadway, high traffic parking lot or building entrance (pedestrian and vehicles)
    - **Existing Soft Landscape (dirt and grass)**
        - Trench width to be 140mm wide and 650mm deep
        - Supply and place 300mm of sand (for pipe bedding)
        - Re-use and place 200mm of native soil
        - Supply and place 150mm of topsoil
    - **Existing Asphalt**
        - Trench width to be 140mm wide and 850mm deep
        - Supply and place 300mm of sand (for pipe bedding)
        - Re-use and place 300mm of native soil
        - Supply and place 150mm of Gravel base
        - Install of 100mm of asphalt to match existing

- **Existing Concrete**
  - Trench width to be 140mm wide and 650mm deep
  - Supply and place 300mm of sand (for pipe bedding)
  - Re-use and place 100mm of native soil
  - Supply and place 150mm of Gravel base
  - Install of 100mm of concrete to match existing
- **Surface mount**
  - On strut with pipe clamps, and ¼" inserts hardware mounted directly to wall (no trapeze or racking)
  - Conduit to be no higher than 14'

DCFC specific scope/specs:

- Storage and handling for up to 30 calendar days from time of receiving at Power Pros Warehouse.
- Supply and shipping of concrete precast 1000mm x 1000mm x 400mm deep
- Excavate hole 1600mm x 1600mm x 575mm deep
- Supply and place 150mm of Gravel base below the precast base
- Place pad, top to be 25mm proud of the surrounding area.
- Supply and place native soil as backfill around the pad to 250mm below grade
- Finish around precast pad to match existing surface as per trench finishing specs.

L2 specific scope/specs:

- Storage and handling for up to 30 calendar days from time of receiving at Power Pros Warehouse.
- Supply and shipping of concrete precast 500mm x 500mm x 1000mm deep
- Excavate hole 1100mm x 1100mm x 1125mm deep
- Supply and place 150mm of Gravel base below the precast base
- Place pad, top to be 25mm proud of the surrounding area.
- Supply and place native soil as backfill around the pad to 250mm below grade
- Finish around precast pad to match existing surface as per trench finishing specs.

Kiosk specific scope/specs:

- Single ground plate and main ground connection
- Single 4" DBII 90'd and stubbed 1m outside of kiosk perimeter underground as per BC Hydro standards
- Coordination with city facility for pickup
- Supply and shipping of concrete precast for single DCFC or L2 Kiosk, 1100mm x 1100mm x 400mm deep
  - Excavate hole for above pad 1700mm x 1700mm x 450mm deep
- Supply and shipping of concrete precast for 2-3 DCFC, 2900mm x 1200mm x 300mm deep
  - Excavate hole for above pad 3500mm x 1800mm x 350mm deep
- Supply and place 150mm of Gravel base below the pad
- Place pad, top to be 100mm proud of the surrounding area.
- Supply and place native soil as backfill around the pad to 250mm below grade
- Finish around precast pad to match existing surface as per trench finishing specs.

Exclusions:

***Below is a list for scope of work that we have excluded from our pricing. This is because the item is either not needed on most projects, is over and above code requirements, or the cost may be based on specific requirements that are unique to the site design (which has not been produced yet). Once a design is complete and scope of work is determined, we will be happy to provide any of these items and the additional pricing if deemed necessary**

- Hydrovac
- Hard clay excavation
- Large Rocks and boulders in trench
- Gravel finishes
- Sod or seeding in topsoil
- Removal of large shrubs, plants, bushes, trees
- Replacement of all shrubs, plants, bushes, trees
- Extra costs due to concrete under existing asphalt as sometimes found in city of Vancouver roadways.
- Monolithic or standard curb, or vehicle let down forming and pouring concrete
- Supply and install of pull boxes or service boxes
- Angled trenches through roadways. All trenching assumed to be parallel or perpendicular to roadway
- Lap joints in asphalt or concrete finishing
- Decorative concrete
- Engineered or structural fill
- Additional fill required if native soil does not meet spec'd requirements (where native soil has been listed as to be reused for backfill)
- Concrete encased conduits or ducts
- Protective Bollards or Bump stops
- Sign and sign base supply or installation
- Pour in place and reinforcing steel bases for equipment
- Painting or road markings
- Custom coatings
- Exploratory Work and site assessment
- Review of potential underground conflicts
- Surveying
- X-ray scanning (general utility scanning and BC One Call allowed for)
- Street Sweeper
- Project operational costs during time waiting for engineer inspections and/or testing of trench, city inspection, arborist, archeologist, contaminated soils testing, or other third party
- Arborist and Arborist tree protection requirements
- Tree root blocking membrane or other underground
- Archeologist
- Environmental issues, management plan, reporting, monitoring, testing, remediation.
- Temporary storm water treatment and discharging of storm water offsite.
- Erosion, water runoff, and sediment control
- Asbestos testing
- Abatement of working area

- Heights unable to be accessed by 12' ladder (scaffolding or man-lift required)
- Engineer and/or as-built drawings
- Consultant
- Geotech
- Flagging
- Design time
- Project Management
- Contaminated soils testing
- Contaminated soil dumping
- Japanese beetle dumping or reporting costs
- Repairs or rerouting of existing utilities.
- Temporary pedestrian control walkways, let down, or wheelchair accessibility infrastructure
- On Site Security
- Hoarding
- Traffic management Signage
- Washroom
- COVID Safety and/or wash station
- First Aid above level 1
- Site Trailer
- Temporary power, water, or lighting
- Trash pump and excavation delays due to water egress in trench
- Winter Work (Snow, Ice, Frozen ground conditions)
- Extreme Weather
- Snow clearing
- Temporary heating
- Permit application and costs
- Liquidated damages/late completion/penalty clauses
- Force Majeure delays including any on site or local pandemic or virus/disease breakout
- Repairs of damages caused by excavator operation, offloading and onloading
- Temporary ramps or driveways for excavator or construction vehicles required due to site specifics
- Steel Road Plate
- Arc-Flash Study
- Megger testing
- Distribution equipment changes when installing charging equipment off existing building power.
- Distribution kiosk supply or storage
- Changes or additions to Kiosk (only placement, mounting hardware install, and terminations of field conductors allowed for)
- Delays due to kiosk supply or pickup access by provided by City of Vancouver
- Delays due to DCFC or L2 supply provided by Greenlots
- Delays or changes caused by any equipment, materials, or scope not provided by Power Pros Electrical.
- Utility Design coordination with BC Hydro and/or other
- Any third-party metering, communication equipment, surge suppression equipment, and other specific electrical equipment supply and installation, not included within DCFC or L2 equipment.
- Storage and handling beyond 30 calendar days from time of receiving at Power Pros Warehouse.
- Special insurance requirements beyond general liability.

- Additional costs for overtime outside of regular business hours (Mon-Fri, 40-hour work weeks, between the hours of 7:00AM – 5:00PM, excluding holidays)
- Additional costs which **may** be required due to projects requested to be started within 60 days of provided IFC drawings.
- Bonding

*Power Pros reserves the right to re-negotiate pricing due a major unforeseen increase in cost due to uncontrollable world events causing major increase in costs above 10% in any calendar year. This would include events such as natural disasters, international trade tariffs, international supply shortages, major economy/market adjustments, etc. Power Pros will be required to show documentation justifying price increases for any re-negotiations to be approved.

Additional Rates:
EV consulting, design, and project management provided on a per hour basis (pricing in spreadsheet)

Respectfully Submitted,
PowerPros Electrical Ltd.

Steve Abercromby
Manager – EV Infrastructure

SCHEDULE C -
DEPLOYMENT PLAN

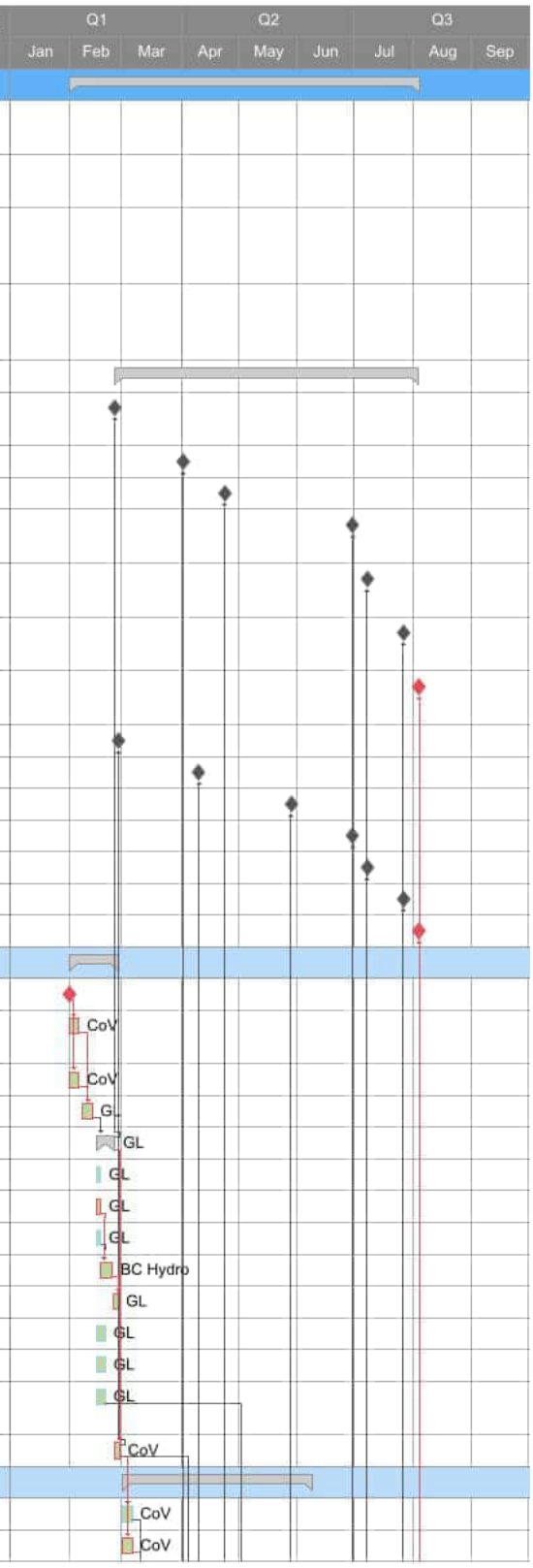
Three (3) pages

Schedule C – Deployment Plan

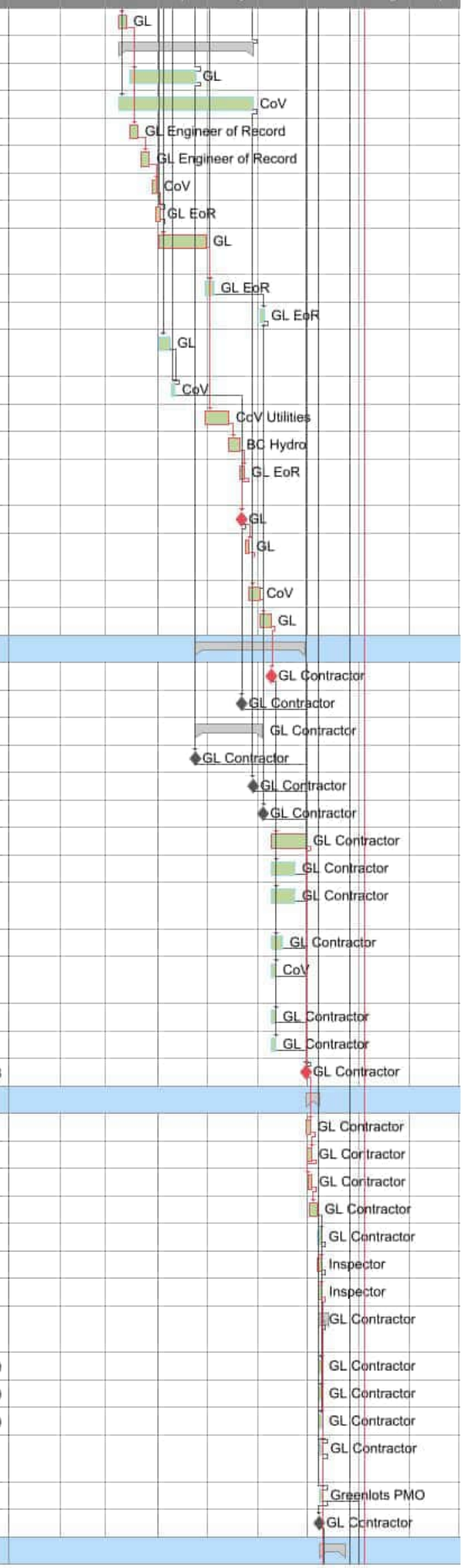
smartsheet

This schedule represents an illustrative timeline for the ordering, delivery, installation, commissioning, testing, acceptance of 1 EV station and any other necessary steps that need to be completed by Supplier (with input by the City where shown)

	Task Name	Duration	Predecessors
1	Site X	131.95d	
2	*Dates shown are for illustration only and will depend on the Start milestone date for any particular project*		
3	*This illustrative timeline assumes that where input is required of the City, the City will provide such input within a reasonable period of time.*		
4	*The Supplier will ensure it has sufficient resources to reasonably meet this timeline if the City directs Supplier to deploy more than one station concurrently.*		
5	** Row for controlling Baseline finish dates (for site level parent row conditional formatting of columns [Site Acquisition Finish] to [Close-Out Finish]): Green: On Schedule, Yellow: <=1 week behind, red: >1 week behind **	N/A	N/A
6	Milestones Table	113.95d	
7	Key Milestone 1: 2w BfD dev. (from CoV REFM buy-in and data delivery to BfD IFA (w or w/o BC Hydro information))	0	26
8	Key Milestone 2: 4w IFB dev. (from BfD approval to IFB)	0	46
9	Key Milestone 3: xw Long Lead Del. (from OEM PO to Delivery)	0	41
10	Key Milestone 4: xw Construction Prep. (from Construction PO issuance to Mobilization date in PO)	0	73
11	Key Milestone 5: xw Ready for Energization (from Mobilization to Mechanically Complete date in PO)	0	86
12	Key Milestone 6: 1w Commissioned (from Energization to Commissioning) (Ready for Normal Operations)	0	106
13	Key Milestone 7: 4w Close Outs (from Commissioning to Turnover and final non-critical punches, season dependent)	0	118
14	Basis for Design Approved	0	35
15	Final Investment Decision	0	51
16	Long Leads Delivered (EVSEs, Kiosks)	0	40
17	Ready for Construction	0	73
18	Site Mechanically Complete	0	87
19	Site Commissioned	0	105
20	Site Closed-Out	0	118
21	Site Assessment	20d	
22	Start	0	
23	Establish buy-in with Real Estate & Facilities Management (REFM) to assess site	5d	22
24	Site data collection	5d	22
25	Site Assessment	5d	24, 23
26	Develop Basis for Design (BfD)	8d	25
27	Site Assessment Report incl. surveys recommendations	2d	
28	Preliminary site plan	2d	
29	Preliminary Single Line Diagram incl. EVSE & Kiosk selections	2d	
30	BC Hydro prelim feasibility check	5d	28, 29
31	Update Preliminary site plan & SLD w BC Hydro feedback if any	1d	30
32	GL Scope Preliminary cost estimate	5d	
33	Detailed quote for engineering & surveys	5d	
34	Design Specifications (incl. standard CoV Kiosk specs, shop drawings, and Kiosk pad specs to integrate into rest of design)	5d	
35	Review & Approve BfD	2d	26
36	Engineering & Procurement	72d	
37	Issue Kiosk PO to Kiosk Vendor	5d	35
38	Issue Engineering, Surveys & Long Lead PO to GL	5d	35



	Task Name	Duration	Predecessors
39	Issue Engineering, Surveys & Long Lead POs to contractors and OEMs	5d	38
40	Long Lead Procurement (EVSEs, Kiosks)	60d	
41	EVSEs (unbranded)	6w	39
42	Kiosk	12w	37
43	Surveys	5d	39
44	Engineering & Issue IFR 90%	5d	43
45	Review IFR	2d	44
46	Engineering & Issue IFB 95% (up to point of connection on Kiosk)	2d	45
47	Coordinating BC Hydro interconnection design incl. providing arc flash inputs (if required ex. fast chargers) & cost estimate	4w	35, 46
48	Produce Arc Flash Study	3d	47, 34
49	Produce and Send Arc Flash labels to contractor	2d	48, 57
50	RFP with preferred contractors (incl. civil for BC Hydro which is not engineered by GL EoR)	5d	46
51	Review & Select winning bid	0.5d	50
52	BC Hydro Prelim IFC Utilities Review	10d	47
53	BC Hydro implements any Utilities Review Changes	5d	52
54	Review BC Hydro design and incorporate interconnection civil scope into IFC as needed	1d	53
55	Issue IFC 100%	0	51, 54
56	Reconcile any BC Hydro change impacts with contractor bid. (MOC with CoV)	2d	55
57	Issue Construction PO to GL	5d	56
58	GL Issue POs to contractor	5d	57
59	Pre-Construction	47d	
60	Construction PO received from Greenlots	0	58
61	Receive IFC package from Engineering	0	55
62	Receive Free Issue Materials	29d	
63	EVSEs (unbranded)	0	41
64	Kiosks	0	42
65	Arc Flash Warning Labels	0	49
66	Procure Balance of Plant	3w	60
67	Get Construction Permits & Locates	10d	60
68	Get special permits if needed (ex. building permit, temporary special zone)	10d	60
69	Confirm Greenlots Permit to Work System and JSA implemented	5d	60
70	Confirm readiness w stakeholders: Facilities Management Readiness (if at city facility other than curbside), Park Board (if at park)	1d	60
71	Schedule electrical inspections with CoV inspector	1d	60
72	Schedule Utility Work with BC Hydro (if DCFCs involved)	1d	60
73	Joint Final Construction Readiness Meeting (w GL and CoV)	0	63, 64, 68
74	Construction	6d	
75	Mob 1	0.5d	73
76	Construction	1d	75
77	Trench inspection by city electrical inspector	0.1d	76FF
78	Construction (continued)	3d	77
79	Walkdown w Greenlots' Mechanical Completions QC Checklist	0.5d	78
80	Electrical inspection by city electrical inspector	0.5d	78
81	Electrical Inspector's Connection Authorization	0.5d	80
82	Close-out deficiencies and review before/after photo evidence progressively with Greenlots	0.5d	
83	Deficiency 1 (attach photos of before and after)	0.5d	79, 78, 80
84	Deficiency 2 (attach photos of before and after)	0.5d	79, 78, 80
85	Deficiency N (attach photos of before and after)	0.5d	79, 78, 80
86	Certify and Issue Mechanical Completion Certificate to Greenlots via Docusign	2h	82, 81
87	Greenlots reviews and executes Mechanical Completion Certificate	2h	86
88	Demob 1 (if DCFC and BC Hydro needed but scheduled for different day)	0	87
89	Energization	12.2d	



	Task Name	Duration	Predecessors	Q1			Q2			Q3		
				Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep
90	Source CCS type 1 or CHAdeMO EV (or PHEV) for onsite commissioning support	1d	88							GL Contractor		
91	Track BC Hydro Mob Date (if needed and adjust as necessary)	10d	81							GL Contractor		
92	Schedule interconnection and final inspection date with BC Hydro and city inspector	0.2d	91SS							GL Contractor		
93	BC Hydro Mob	0	91							BC Hydro		
94	Track BC Hydro Construction (if needed, adjust as necessary)	1d	93							GL Contractor		
95	Schedule commissioning step with Greenlots	0	102SF -4c							GL Contractor		
96	Collect Onboarding Information (precommissioning)	1d	95							Greenlots CX Tea		
97	Mob 2 incl. EV or PHEV for commissioning support	0.5d	98SF, 90							GL Contractor		
98	Interconnection	0.5d	94FF							GL Contractor		
99	City inspector final inspection	0.5d	98, 92							City Inspector		
100	City inspector Certificate of Inspection	0.5d	99							City Inspector		
101	Energization	0.2d	100							GL Contractor		
102	Initiate commissioning step with Greenlots and get ready to support with EV or PHEV testing on site. DO NOT DEMOB	0	101							GL Contractor		
103	Commissioning	1.25d										
104	Remote Commissioning by Greenlots	1d	96, 102							Greenlots CX T		
105	Contractor provides on-site commissioning support to Greenlots with PHEV and functional tests (1 day allowance)	1d	104SS, 10							GL Contractor		
106	Site Commissioned	0	104							Greenlots CX T		
107	Demob 2	0	106							GL Contractor		
108	Produce Operations Readiness Report	2h	106							Greenlots CX T		
109	Close-out	6.25d										
110	provide final redlines to Greenlots	2d	107							GL Contractor		
111	Return panel padlock keys to Greenlots	2d	107							GL Contractor		
112	As-builts by Engineering	2d	110							GL EoR		
113	Close special permits if applicable (ex. building permit Subsection 2.2.7., Division C of the Building By-law)	1d	87, 110							GL EoR		
114	Compile turn-over package of (1) Mechanical Completion Certificate, (2) As-Builts, (3) Certificates of Inspection, (4) Operational Readiness Report	2h	112, 113							Greenlots PMC		
115	Issue turn-over package to client	0	114							Greenlots PMC		
116	Send Customer Acceptance Certificate to client via Docusign	0	115							Greenlots PMC		
117	Client Executes and returns Final Acceptance Certificate to Greenlots	2d	116							CoV		
118	Site is turned over	0	117							Greenlots PM		
119												
120												
121												

SCHEDULE D –
PCI REQUIREMENTS

Compliance with PCI Data Security Standards

For purposes of this Schedule D, each capitalized term will have the meaning given in the Agreement except if it is defined as follows or defined in the body of this schedule:

(i) "Greenlots Acquirer" refers to Supplier's acquirer, PayPal Inc. (Braintree).

(ii) "Attestation of Compliance" or "AOC" shall mean a form for merchants and service providers to attest to the results of a PCI Data Security Standards assessment, as documented in the Self-Assessment Questionnaire or Report on Compliance (as such terms are defined in the PCI Data Security Standards). Note, only official AOC documents which are specifically provided by PCI Security Standards Council for demonstrating compliance will be accepted as evidence of compliance. Third-party certificates will not be accepted.

(iii) "Card Brand" means organizations providing Payment Card services. Organizations include, but are not limited to, MasterCard, Visa, American Express, Discover, and JCB.

(iv) "Cardholder" means the consumer who owns and utilizes the Payment Card to purchase electric vehicle charging services from the City.

(v) "Cardholder Data" refers to primary account number, Cardholder name, expiration date and/or service code, and security-related information (including but not limited to card validation codes/values, full track data, PINs and PIN blocks) used to authenticate Cardholders and/or authorize Payment Card transactions;

(vi) "Cardholder Data Services" means services provided by Supplier to the City, as reflected in the attached diagram attached as Appendix 1 to this Schedule X, that are directly involved in transmitting, processing or storing Cardholder Data on behalf of the City or that control or could impact the security of Cardholder Data or possession of Cardholder Data by Supplier on behalf of the City;

(vii) "Card-Present Transactions" means transactions where both the Payment Card and the Cardholder are present at the point of sale, in this case, at a Charging Unit.

(viii) "Charging Unit" has the meaning given to such term in Schedule H – Terms and Conditions relating to O&M Services.

(ix) "City's Acquirer" refers to the City's acquirer, Moneris.

(x) "Compromised Data Event" means any reasonably suspected, reasonable allegation of or actual loss, disclosure, theft or compromise of Cardholder Data or Payment Card transaction information.

(xi) "ISA" means an Internal Security Assessor that has been qualified by the PCI Security Standards Council.

(xii) "Merchant Account" means the account assigned to Supplier (as defined in PCI Data Security Standards) by Greenlots Acquirer (as defined in PCI Data Security Standards).

(xiii) "Online Payment Gateway" refers to online payment gateway technology provided by Supplier to customers, including Supplier's mobile application and the online website (https://charge.greenlots.com).

(xiv) "Payment Card" means electronic payment cards such as credit, debit or pre-paid debit cards used to purchase services or goods.

(xv) "Payment Processor" means Supplier's Payment Card processing service provider. On the date

of the Agreement, the Payment Processor is Paypal Inc. (Braintree).

(xvi) "PCI Data Security Standards" or "PCI DSS" means the PCI Data Security Standards and any successor standards and requirements developed by PCI Security Standards Council.

(xvii) "QSA" means an independent Qualified Security Assessor organization that has been qualified by the PCI Security Standards Council to validate an entity's adherence to PCI DSS.

(xviii) "SAQ" mean Self-Assessment Questionnaire, a reporting tool used to document self-assessment results from an entity's PCI DSS assessment.

(xix) "SKY Platform" means Suppliers' SKYTM software-as-a-service platform made available to the City pursuant to the SKY Subscription Terms.

(xx) "SKY Subscription Terms" means terms and conditions relating to use of the SKY Platform by the City, the terms of which are set out in Schedule G - Terms and Conditions relating to Software to the Agreement.

A. PCI Acknowledgment. Supplier acknowledges its understanding of the PCI Data Security Standards and the importance of Cardholder data security and that Supplier is responsible for (i) the security of Cardholder data that it possesses, has been given access to, stores, or transmits on behalf of the City; (ii) providing all Cardholder data payment processing services for every Merchant Account for which it is processing such payments; and (iii) managing and complying with all applicable PCI Data Security Standards. Supplier shall at all times comply with all applicable PCI Security Standards.

B. PCI Certification. Supplier represents and warrants to the City that Supplier is certified as a Level 2 Service Provider in accordance with PCI Data Security Standards (or any successor certification established under PCI Data Security Standards) and covenants that it will, for the duration of the Term of the Agreement, continuously maintain and comply with all applicable requirements of such certification. If, any time during the Term of the Agreement, Supplier's transaction volumes require a Level 1 Service Provider certification pursuant to PCI Data Security Standards, Supplier will, without delay, carry out the steps required by PCI Data Security Standards for a Level 1 audit and certification.

C. QSA Requirement. For the duration of the Term of the Agreement, Supplier agrees that it will engage a QSA to review, approve and sign off on the Supplier's PCI Compliance AOCs and SAQs in accordance with PCI Data Security Standards.

D. SureCall QSA Audit. Supplier covenants that their current call center service provider, SureCall, will be going through a PCI-DSS Audit with a QSA. This audit will commence in early January 2021 with planned completion and certification anticipated by the end of June 2021. If Supplier proposes to change its call center service provider during the Term of the Agreement, Supplier shall, if required by PCI Data Security Standards, give the required advance notice to the City and, even if not required, give as much advance written notice to the City as reasonably possible. Supplier shall, in addition to any reasonable requests from the City and any Supplier obligations under PCI Data Security Standards, cause a new call center service provider to undergo a PCI-DSS Audit with a QSA and be certified in accordance with this Section D.

E. Temporary Call Center Payment Solution. Supplier's standard call center script and resolution process dictates that if any driver is unable to initiate charging session with payment via RFID or the Supplier's mobile app, drivers can provide their credit card information by phone, to Supplier's call center service provider. Until the SureCall QSA audit referenced in Section D, is complete, Supplier agrees to modify its standard call center script and resolution process as follows:

(i) In the event that any Charging Units go live within the City, on the Supplier's network, prior to SureCall achieving certification described in Section D, and a driver needs to

make payment via the telephone, SureCall will inform the driver that there would be no charge for their charging session.

(ii) In this event, SureCall would allow the charging session at no charge to the driver. Supplier will track all such no-charge sessions, as part of this temporary solution. Supplier will provide the City monthly reimbursements that cover the energy cost for each of these charging sessions.

(iii) The cost of charging sessions will be owned by the Supplier until a time when SureCall has received the certification described in Section D, to accept payment information over the telephone. At such time, SureCall representatives will then accept credit card information by telephone, to initiate and transact for these charging sessions.

F. Card Brand Requirements. Supplier is responsible to ensure, at its cost, that the SKY Platform and Supplier provided hardware involved in provisioning services under the Agreement is configured and updated with all appropriate security patches, revisions, mandates, and other updates as required by the Card Brands, Payment Processor, and PCI Data Security Standards or as required by the City in connection with similar requirements imposed on the City by the Card Brands and PCI Data Security Standards.

G. Payment Processor. Supplier agrees that it will, during the Term of the Agreement, (i) continuously have a legally enforceable contract with a Payment Processor, and (ii) ensure that the Payment Processor complies with its, and Supplier's, obligations under PCI Data Security Standards. If Supplier proposes to change its Payment Processor during the Term of the Agreement, Supplier shall, if required by PCI Data Security Standards, give the required advance notice to the City and, even if not required, give as much advance written notice to the City as reasonably possible. Supplier shall, in addition to any reasonable requests from the City and any Supplier obligations under PCI Data Security Standards, cause a new Payment Processor to undergo a PCI-DSS Audit and certification process with a QSA.

H. Examinations and Audits. Supplier agrees that the City may examine or audit the material records and operations of Supplier provided (i) the City gives Supplier reasonable advance written notice of such examination or audit, (ii) in the City's written notice, the City notifies Supplier of the reason for such examination or audit, which reason may include a change in Supplier's Payment Processor, a material change to the PCI DSS which impacts Supplier, a change in Supplier's Acquirer, a change in any other Supplier service provider as contemplated in Section I (ii) below, a change in merchant requirements, a change in Card Brand requirements, change in Supplier's payment call centre service provider or any other reasonable grounds for the City to conduct an examination or audit, and (iii) the City conducts such examination or audit itself or uses the City's ISA, the City's QSA or a recognized expert in the industry to conduct such examination or audit. The City and Supplier will work together, acting reasonably, to ensure that the scope, costs and expenses related to any such examination or audit are reasonable. The City acknowledges and agrees that if it requests an examination or audit as provided in this Section H more frequently than once per calendar year (unless a Compromised Data Event has occurred), the City will be responsible for the costs and expenses of any such examination or audit.

I. Notifications or Written Records by Supplier. Supplier shall provide, at its expense and subject to the City's confidentiality obligations under ARTICLE 15 of the Agreement, written notice or written records to the City's PCI Office by e-mail to PCI.Compliance@Vancouver.ca as follows:

(i) Supplier must provide its AOC annually on or prior to the annual expiry,

(ii) Supplier must provide a letter in the form set out in Appendix 3, together with the required submissions, at the times set out in Appendix 3,

(iii) Upon the City's request, acting reasonably, Supplier must provide copies of certain written records required to be submitted by Supplier under PCI-DSS requirements, and

(iv) Supplier must notify the City with reasonable advanced written notice of any change to its service providers within the scope of Supplier's PCI DSS requirements, and scope of

the electric vehicle charging services Supplier is providing to the City under the Agreement. Service providers in scope include but are not limited to the Payment Processor and payment call centre operator. This written notice shall be e-mailed to the City's PCI Office in accordance with the above and copied to the City in accordance with the notice section of the Agreement.

J. Charging Units. Supplier will not enable Card-Present Transactions to occur at a Charging Unit unless requested by the City in writing. Regardless whether or not Card-Present Transactions occur at a Charging Unit, Supplier is responsible for inspecting Charging Units for signs of damage, malfunction, or tampering of any nature including physical or electronic in accordance with Supplier's service level commitments set out in Schedule H – Terms and Conditions relating to O&M Services of the Agreement. If Supplier or Supplier's Subcontractor observes any signs of damage, malfunction, or tampering with such Charging Unit which could reasonably lead to a Compromised Data Event, Supplier shall report such condition to the City as outlined in Section K. If Card-Present Transactions are permitted at a Charging Unit and Supplier and the City agree on service level commitments for such Charging Unit that are different from the service level commitments initially set out in Schedule H – Terms and Conditions relating to O&M Services, Supplier shall comply with the latest set of agreed service level commitments.

K. Notice of Compromised Data Event. In the event of a Compromised Data Event, Supplier shall within forty-eight (48) hours of becoming aware of such Compromised Data Event notify (i) the City's PCI Office by sending an email to PCI.Compliance@Vancouver.ca, (ii) the Office of the Treasurer by sending an email to abtreasury@vancouver.ca, and (iii) in the manner required in the PCI Data Security Standards, applicable law and the notice section of the Agreement. Supplier shall cooperate with any examinations or audits in accordance with Section H. Upon a Compromised Data Event, Supplier will not alter or destroy any related records and will maintain complete and accurate documentation regarding any modifications made to the records for the period required by applicable law.

L. Business Continuity. Supplier shall maintain reasonable and appropriate business continuity procedures and systems to ensure continuous security of Cardholder Data and compliance with all applicable PCI Security Standards in the event of a disruption, disaster or failure of Supplier's systems.

M. Compliance with Applicable Law. Supplier shall, and shall require all of its sub-contractors to, comply with all applicable Laws including, without limitation, Laws relating to Cardholder Data and Cardholder Data Services and Applicable Privacy Laws.

N. Term of Compliance. Supplier shall comply with the terms of this Schedule D for the entire Term of the Agreement.

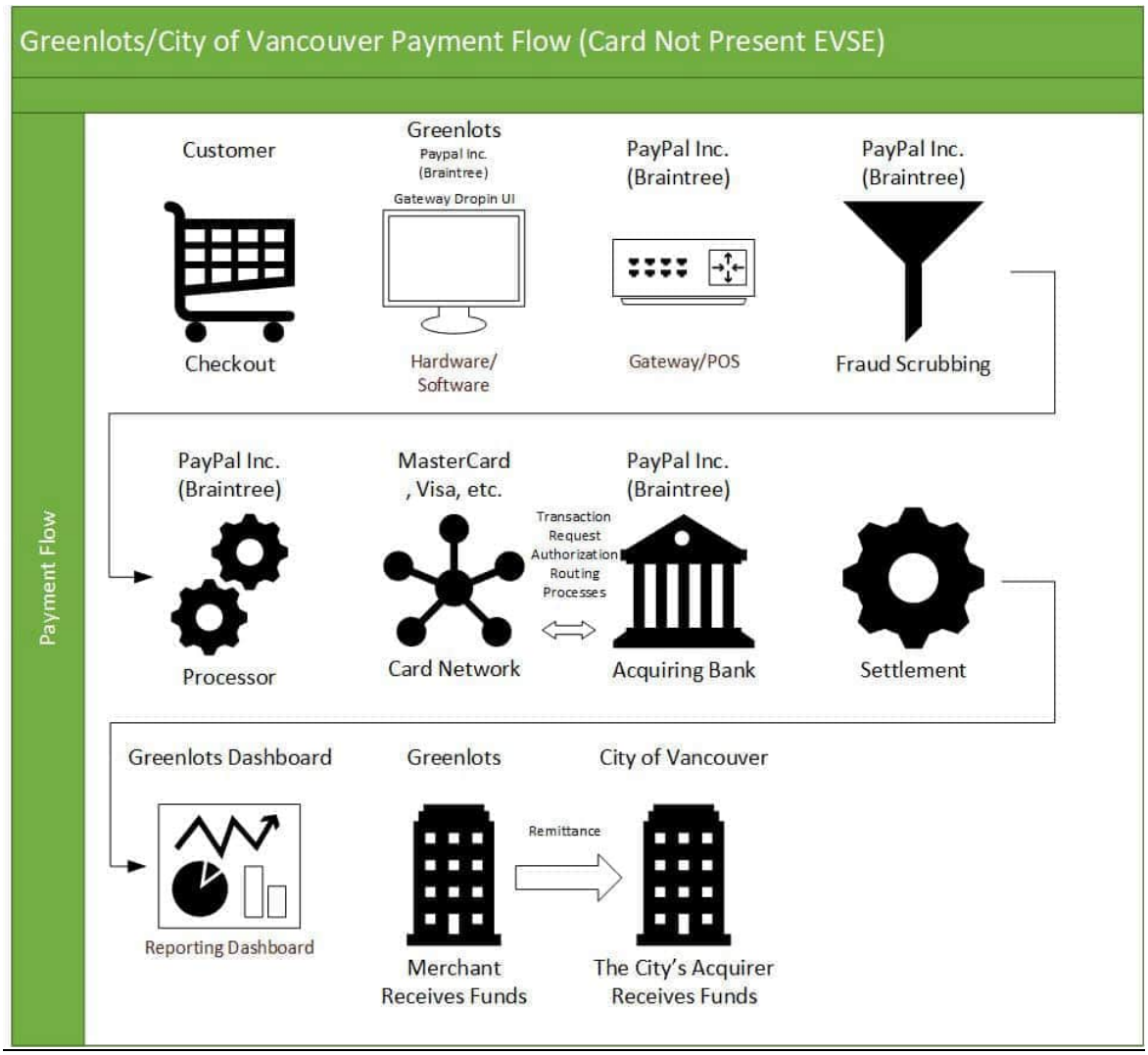
O. Further Indemnity. Without limiting the scope of, and supplemental to and in accordance with the indemnification procedures and liability limits set forth in the Agreement, Supplier's indemnity obligations under the Agreement, Supplier further agrees to indemnify the City for (i) any fines, penalties or other amounts imposed on the City in connection with PCI Data Security Standards in connection with the Agreement, or (ii) any incremental costs incurred by the City in order for the City to rectify any Supplier breach of, or Supplier failure to comply with, Supplier's obligations relating to PCI Data Security Standards under the Agreement.

P. Responsibility Matrix. The City and Supplier agree to the terms of the Responsibility Matrix attached hereto as Appendix 2 and further agree to update such terms as necessary by written agreement.

SCHEDULE D – APPENDIX 1
CARDHOLDER DATA SERVICES AND CASHFLOW DIAGRAM

Diagram – Cardholder Data Services and Cashflow

The diagram below describes the flow of cash throughout Supplier's payment channels and how cash is distributed to other parties.



SCHEDULE D – APPENDIX 2
PCI DSS RESPONSIBILITY MATRIX

Supplier Responsibility Matrix

Attached below as 'Appendix 2 - PCI_DSS Responsibility Matrix_updated_20200715_sal' is the Responsibility Matrix provided by Supplier to the City on July 15th, 2020, which outlines PCI DSS responsibilities between Supplier, Supplier's Subcontractors, and the City.

Note: the Excel Matrix is provided as an attachment in this electronic executed PDF copy of the Agreement.

PCI DSS 3.2.1 Management Responsibility Matrix Between Zeco Systems, Inc. dba Greenlots and City of Vancouver	
The purpose of this spreadheet is to satisfy PCI DSS Requirement 12.8.5: Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	This document is intended to meet the requirements for PCI DSS V3.2.1 Requirement 12.8.5 as it relates to the Payment Processing service provided by Greenlots. As such, the following list of controls and applicable responsibilities only apply to the security of cardholder data which is accepted by the Greenlots' SKY Software on behalf of City of Vancouver. This document does not apply to any cardholder data that City of Vancouver processes, stores, transmits, or otherwise uses for any other purpose, or on the behalf of any other entities. Note: Please leave row blank for not applicable.

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Firewalls are devices that control computer traffic allowed between an entity's networks (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within an entity's internal trusted networks. The cardholder data environment is an example of a more sensitive area within an entity's trusted network.

A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.

Other system components may provide firewall functionality, as long as they meet the minimum requirements for firewalls as defined in Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of Requirement 1.

PCI DSS Control Details			Control Responsibility				
PCI DSS Requirement	**Testing Procedure**	**Guidance**	**100% Service Provider**	**100% City of Vancouver**	**Shared**	**N/A**	**Please provide additional details where the City of Vancouver's PCI Environment may be impacted.**
Are firewall and router configuration standards established and implemented to include the following:							
1.1 Establish and implement firewall and router configuration standards that include the following:	1.1 Inspect the firewall and router configuration standards and other documentation specified below and verify that standards are complete and implemented as follows:	Firewalls and routers are key components of the architecture that controls entry to and exit from the network. These devices are software or hardware devices that block unwanted access and manage authorized access into and out of the network. Configuration standards and procedures will help to ensure that the organization's first line of defense in the protection of its data remains strong.	YES				Greenlots application is hosted on AWS and the firewall and router infrastructure is provided and maintained by AWS. White listed IP and blackllisted IP are done via approvals only.
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	1.1.1.a Examine documented procedures to verify there is a formal process for testing and approval of all: - Network connections, and - Changes to firewall and router configurations 1.1.1.b For a sample of network connections, interview responsible personnel and examine records to verify that network connections were approved and tested. 1.1.1.c Identify a sample of actual changes made to firewall and router configurations, compare to the change records, and interview responsible personnel to verify the changes were approved and tested.	A documented and implemented process for approving and testing all connections and changes to the firewalls and routers will help prevent security problems caused by misconfiguration of the network, router, or firewall. Without formal approval and testing of changes, records of the changes might not be updated, which could lead to inconsistencies between network documentation and the actual configuration.	YES				Greenlots application is hosted on AWS and the firewall and router infrastructure is provided and maintained by AWS. White listed IP and blackllisted IP are done via approvals only.
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	1.1.2.a Examine diagram(s) and observe network configurations to verify that a current network diagram exists and that it documents all connections to cardholder data, including any wireless networks. 1.1.2.b Interview responsible personnel to verify that the diagram is kept current.	Network diagrams describe how networks are configured, and identify the location of all network devices. Without current network diagrams, devices could be overlooked and be unknowingly left out of the security controls implemented for PCI DSS and thus be vulnerable to compromise.	YES				
1.1.3 Current diagram that shows all cardholder data flows across systems and networks	1.1.3 Examine data-flow diagram and interview personnel to verify the diagram: - Shows all cardholder data flows across systems and networks. - Is kept current and updated as needed upon changes to the environment.	Cardholder data-flow diagrams identify the location of all cardholder data that is stored, processed, or transmitted within the network. Network and cardholder data-flow diagrams help an organization to understand and keep track of the scope of their environment, by showing how cardholder data flows across networks and between individual systems and devices.	YES				
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	1.1.4.a Examine the firewall configuration standards and verify that they include requirements for a firewall at each Internet connection and between any DMZ and the internal network zone. 1.1.4.b Verify that the current network diagram is consistent with the firewall configuration standards. 1.1.4.c Observe network configurations to verify that a firewall is in place at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone, per the documented configuration standards and network diagrams.	Using a firewall on every Internet connection coming into (and out of) the network, and between any DMZ and the internal network, allows the organization to monitor and control access and minimizes the chances of a malicious individual obtaining access to the internal network via an unprotected connection.	YES				

1.1.5 Description of groups, roles, and responsibilities for management of network components	1.1.5.a Verify that firewall and router configuration standards include a description of groups, roles, and responsibilities for management of network components 1.1.5.b Interview personnel responsible for management of network components to confirm that roles and responsibilities are assigned as documented.	This description of roles and assignment of responsibilities ensures that personnel are aware of who is responsible for the security of all network components, and that those assigned to manage components are aware of their responsibilities. If roles and responsibilities are not formally assigned, devices could be left unmanaged.	YES				
1.1.6 Documentation of business justification and approval for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	1.1.6.a Verify that firewall and router configuration standards include a documented list of all services, protocols and ports, including business justification for each. 1.1.6.b Identify insecure services, protocols, and ports allowed; and verify that security features are documented for each service. 1.1.6.c Examine firewall and router configurations to verify that the documented security features are implemented for each insecure service, protocol, and port.	Compromises often happen due to unused or insecure service and ports, since these often have known vulnerabilities and many organizations don't patch vulnerabilities for the services, protocols, and ports they don't use (even though the vulnerabilities are still present). By clearly defining and documenting the services, protocols, and ports that are necessary for business, organizations can ensure that all other services, protocols, and ports are disabled or removed. Approvals should be granted by personnel independent of the personnel managing the configuration. If insecure services, protocols, or ports are necessary for business, the risk posed by use of these protocols should be clearly understood and accepted by the organization, the use of the protocol should be justified, and the security features that allow these protocols to be used securely should be documented and implemented. If these insecure services, protocols, or ports are not necessary for business, they should be disabled or removed	YES				
1.1.7 Requirement to review firewall and router rule sets at least every six months	1.1.7.a Verify that firewall and router configuration standards require review of firewall and router rule sets at least every six months. 1.1.7.b Examine documentation relating to rule set reviews and interview responsible personnel to verify that the rule sets are reviewed at least every six months.	This review gives the organization an opportunity at least every six months to clean up any unneeded, outdated, or incorrect rules, and ensure that all rule sets allow only authorized services and ports that match the documented business justifications. Organizations with a high volume of changes to firewall and router rule sets may wish to consider performing reviews more frequently, to ensure that the rule sets continue to meet the needs of the business.	YES				
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. *Note: An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage.*	1.2 Examine firewall and router configurations and perform the following to verify that connections are restricted between untrusted networks and system components in the cardholder data environment:	It is essential to install network protection between the internal, trusted network and any untrusted network that is external and/or out of the entity's ability to control or manage. Failure to implement this measure correctly results in the entity being vulnerable to unauthorized access by malicious individuals or software. For firewall functionality to be effective, it must be properly configured to control and/or limit traffic into and out of the entity's network.	YES				
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	1.2.1.a Examine firewall and router configuration standards to verify that they identify inbound and outbound traffic necessary for the cardholder data environment. 1.2.1.b Examine firewall and router configurations to verify that inbound and outbound traffic is limited to that which is necessary for the cardholder data environment. 1.2.1.c Examine firewall and router configurations to verify that all other inbound and outbound traffic is specifically denied, for example by using an explicit "deny all" or an implicit deny after allow statement.	This requirement is intended to prevent malicious individuals from accessing the entity's network via unauthorized IP addresses or from using services, protocols, or ports in an unauthorized manner (for example, to send data they've obtained from within your network out to an untrusted server.) Implementing a rule that denies all inbound and outbound traffic that is not specifically needed helps to prevent inadvertent holes that would allow unintended and potentially harmful traffic in or out.	YES				
1.2.2 Secure and synchronize router configuration files.	1.2.2.a Examine router configuration files to verify they are secured from unauthorized access. 1.2.2.b Examine router configurations to verify they are synchronized—for example, the running (or active) configuration matches the start-up configuration (used when machines are booted).	While the running (or active) router configuration files include the current, secure settings, the start-up files (which are used when routers are re-started or booted) must be updated with the same secure settings to ensure these settings are applied when the start-up configuration is run. Because they only run occasionally, start-up configuration files are often forgotten and are not updated. When a router re-starts and loads a start-up configuration that has not been updated with the same secure settings as those in the running configuration, it may result in weaker rules that allow malicious individuals into the network.	YES				

1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	1.2.3.a Examine firewall and router configurations to verify that there are perimeter firewalls installed between all wireless networks and the cardholder data environment. 1.2.3.b Verify that the firewalls deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	The known (or unknown) implementation and exploitation of wireless technology within a network is a common path for malicious individuals to gain access to the network and cardholder data. If a wireless device or network is installed without the entity's knowledge, a malicious individual could easily and "invisibly" enter the network. If firewalls do not restrict access from wireless networks into the CDE, malicious individuals that gain unauthorized access to the wireless network can easily connect to the CDE and compromise account information. Firewalls must be installed between all wireless networks and the CDE, regardless of the purpose of the environment to which the wireless network is connected. This may include, but is not limited to, corporate networks, retail stores, guest networks, warehouse environments, etc.				YES	The cardholder data environment is housed inside the 3rd party payment processors' data center.
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	1.3 Examine firewall and router configurations—including but not limited to the choke router at the Internet, the DMZ router and firewall, the DMZ cardholder segment, the perimeter router, and the internal cardholder network segment—and perform the following to determine that there is no direct access between the Internet and system components in the internal cardholder network segment:	A firewall's intent is to manage and control all connections between public systems and internal systems, especially those that store, process or transmit cardholder data. If direct access is allowed between public systems and the CDE, the protections offered by the firewall are bypassed, and system components storing cardholder data may be exposed to compromise.	YES				
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	1.3.1 Examine firewall and router configurations to verify that a DMZ is implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	The DMZ is that part of the network that manages connections between the Internet (or other untrusted networks), and services that an organization needs to have available to the public (like a web server). This functionality is intended to prevent malicious individuals from accessing the organization's internal network from the Internet, or from using services, protocols, or ports in an unauthorized manner.	YES				
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	1.3.2 Examine firewall and router configurations to verify that inbound Internet traffic is limited to IP addresses within the DMZ.		YES				
1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)	1.3.3 Examine firewall and router configurations to verify that anti-spoofing measures are implemented, for example internal addresses cannot pass from the Internet into the DMZ.	Normally a packet contains the IP address of the computer that originally sent it so other computers in the network know where the packet came from. Malicious individuals will often try to spoof (or imitate) the sending IP address so that the target system believes the packet is from a trusted source. Filtering packets coming into the network helps to, among other things, ensure packets are not "spoofed" to look like they are coming from an organization's own internal network.	YES				
1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	1.3.4 Examine firewall and router configurations to verify that outbound traffic from the cardholder data environment to the Internet is explicitly authorized.	All traffic outbound from the cardholder data environment should be evaluated to ensure that it follows established, authorized rules. Connections should be inspected to restrict traffic to only authorized communications (for example by restricting source/destination addresses/ports, and/or blocking of content).	YES				
1.3.5 Permit only "established" connections into the network.	1.3.5 Examine firewall and router onfigurations to verify that the firewall permits only established connections into the internal network and denies any inbound connections not associated with a previously established session.	A firewall that maintains the "state" (or the status)for each connection through the firewall knows whether an apparent response to a previous connection is actually a valid, authorized response (since it retains each connection's status) or is malicious traffic trying to trick the firewall into allowing the connection.	YES				
1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	1.3.6 Examine firewall and router configurations to verify that system components that store cardholder data are on an internal network zone, segregated from the DMZ and other untrusted networks.	If cardholder data is located within the DMZ, it is easier for an external attacker to access this information, since there are fewer layers to penetrate. Securing system components that store cardholder data in an internal network zone that is segregated from the DMZ and other untrusted networks by a firewall can prevent unauthorized network traffic from reaching the system component. Note: This requirement is not intended to apply to temporary storage of cardholder data in volatile memory.	YES				

1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties. *Note: Methods to obscure IP addressing may include, but are not limited to:* *- Network Address Translation (NAT)* *- Placing servers containing cardholder data behind proxy servers/firewalls,* *- Removal or filtering of route advertisements for private networks that employ registered addressing,* *- Internal use of RFC1918 address space instead of registered addresses.*	1.3.7.a Examine firewall and router configurations to verify that methods are in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet.	Restricting the disclosure of internal or private IP addresses is essential to prevent a hacker "learning" the IP addresses of the internal network, and using that information to access the network. Methods used to meet the intent of this requirement may vary depending on the specific networking technology being used. For example, the controls used to meet this requirement may be different for IPv4 networks than for IPv6 networks.	YES				
	1.3.7.b Interview personnel and examine documentation to verify that any disclosure of private IP addresses and routing information to external entities is authorized.		YES				
1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include: -Specific configuration settings are defined. - Personal firewall (or equivalent functionality) is actively running. - Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.	1.4.a Examine policies and configuration standards to verify: - Personal firewall software or equivalent functionality is required for all portable computing devices (including company and/or employee-owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. - Specific configuration settings are defined for personal firewall (or equivalent functionality). Personal firewall (or equivalent functionality) is configured to actively run. - Personal firewall (or equivalent functionality) is configured to not be alterable by users of the portable computing devices.	Portable computing devices that are allowed to connect to the Internet from outside the corporate firewall are more vulnerable to Internet-based threats. Use of firewall functionality (e.g., personal firewall software or hardware) helps to protect devices from Internet-based attacks, which could use the device to gain access the organization's systems and data once the device is re-connected to the network. The specific firewall configuration settings are determined by the organization. Note: This requirement applies to employee-owned and company-owned portable computing devices. Systems that cannot be managed by corporate policy introduce weaknesses and provide opportunities that malicious individuals may exploit. Allowing untrusted systems to connect to an organization's CDE could result in access being granted to attackers and other malicious users.	YES				
	1.4.b Inspect a sample of company and/or employee-owneddevices to verify that: - Personal firewall (or equivalent functionality) is installed and configured per the organization's specific configuration settings. - Personal firewall (or equivalent functionality) is actively running. - Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.						
1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.	1.5 Examine documentation and interview personnel to verify that security policies and operational procedures for managing firewalls are: - Documented, - In use, and - Known to all affected parties.	Personnel need to be aware of and following security policies and operational procedures to ensure firewalls and routers are continuously managed to prevent unauthorized access to the network.	YES				

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Malicious individuals (external and internal to an entity) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.

PCI DSS Control Details			Control Responsibility				Please provide additional details where the City of Vancouver's PCI Environment may be impacted.
PCI DSS Requirement	Testing Procedure	Guidance	100% Service Provider	100% City of Vancouver	Shared	N/A	
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters							
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.).	2.1.a Choose a sample of system components, and attempt to log on (with system administrator help) to the devices and applications using default vendor-supplied accounts and passwords, to verify that ALL default passwords (including those on operating systems, software that provides security services, application and system accounts, POS terminals, and Simple Network Management Protocol (SNMP) community strings) have been changed. (Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.)	Malicious individuals (external and internal to an organization) often use vendor default settings, account names, and passwords to compromise operating system software, applications, and the systems on which they are installed. Because these default settings are often published and are well known in hacker communities, changing these settings will leave systems less vulnerable to attack. Even if a default account is not intended to be used, changing the default password to a strong unique password and then disabling the account will prevent a malicious individual from re-enabling the account and gaining access with the default password.	YES				**Example:**The Customer has the responsibility to remove defaults during their baseline configuration process for any in-scope instances.
	2.1.b For the sample of system components, verify that all unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled.						
	2.1.c Interview personnel and examine supporting documentation to verify that: - All vendor defaults (including default passwords on operating systems, software providing security services, application and system accounts, POS terminals, Simple Network Management Protocol (SNMP) community strings, etc.) are changed before a system is installed on the network. - Unnecessary default accounts (including accounts used by operating systems, security software, applications, systems, POS terminals, SNMP, etc.) are removed or disabled before a system is installed on the network.						
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	2.1.1.a Interview responsible personnel and examine supporting documentation to verify that: - Encryption keys were changed from default at installation - Encryption keys are changed anytime anyone with knowledge of the keys leaves the company or changes positions.	If wireless networks are not implemented with sufficient security configurations (including changing default settings), wireless sniffers can eavesdrop on the traffic, easily capture data and passwords, and easily enter and attack the network. In addition, the key-exchange protocol for older versions of 802.11x encryption (Wired Equivalent Privacy, or WEP) has been broken and can render the encryption useless. Firmware for devices should be updated to support more secure protocols.				YES	All cardholder data is transmitted solely from our mobile app(s) over SSL directly to our 3rd party payment proccesors, therefore we never handle the transmission of personally identifyable payment information over wireless networks.
	2.1.1.b Interview personnel and examine policies and procedures to verify: - Default SNMP community strings are required to be changed upon installation. - Default passwords/phrases on access points are required to be changed upon installation.						
	2.1.1.c Examine vendor documentation and login to wireless devices, with system administrator help, to verify: - Default SNMP community strings are not used. - Default passwords/passphrases on access points are not used.						

	2.1.1.d Examine vendor documentation and observe wireless configuration settings to verify firmware on wireless devices is updated to support strong encryption for: - Authentication over wireless networks - Transmission over wireless networks.						
	2.1.1.e Examine vendor documentation and observe wireless configuration settings to verify other security-related wireless vendor defaults were changed, if applicable.						
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: - Center for Internet Security (CIS) - International Organization for Standardization (ISO) - SysAdmin Audit Network Security (SANS) Institute - National Institute of Standards Technology (NIST).	2.2.a Examine the organization's system configuration standards for all types of system components and verify the system configuration standards are consistent with industry-accepted hardening standards.	There are known weaknesses with many operating systems, databases, and enterprise applications, and there are also known ways to configure these systems to fix security vulnerabilities. To help those that are not security experts, a number of security organizations have established system-hardening guidelines and recommendations, which advise how to correct these weaknesses. Examples of sources for guidance on configuration standards include, but are not limited to: www.nist.gov, www.sans.org, and www.cisecurity.org, www.iso.org, and product vendors. System configuration standards must be kept up to date to ensure that newly identified weaknesses are corrected prior to a system being installed on the network.	YES				
	2.2.b Examine policies and interview personnel to verify that system configuration standards are updated as new vulnerability issues are identified, as defined in Requirement 6.1.						
	2.2.c Examine policies and interview personnel to verify that system configuration standards are applied when new systems are configured and verified as being in place before a system is installed on the network.						
	2.2.d Verify that system configuration standards include the following procedures for all types of system components: - Changing of all vendor-supplied defaults and elimination of unnecessary default accounts - Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server - Enabling only necessary services, protocols, daemons, etc., as required for the function of the system - Implementing additional security features for any required services, protocols or daemons that are considered to be insecure - Configuring system security parameters to prevent misuse - Removing all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.						
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) *Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.*	2.2.1.a Select a sample of system components and inspect the system configurations to verify that only one primary function is implemented per server.	If server functions that need different security levels are located on the same server, the security level of the functions with higher security needs would be reduced due to the presence of the lower-security functions. Additionally, the server functions with a lower security level may introduce security weaknesses to other functions on the same server. By considering the security needs of different server functions as part of the system configuration standards and related processes, organizations can ensure that functions requiring different security levels don't co-exist on the same server.	YES				
	2.2.1.b If virtualization technologies are used, inspect the system configurations to verify that only one primary function is implemented per virtual system component or device.						
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	2.2.2.a Select a sample of system components and inspect enabled system services, daemons, and protocols to verify that only necessary services or protocols are enabled.	As stated in Requirement 1.1.6, there are many protocols that a business may need (or have enabled by default) that are commonly used by malicious individuals to compromise a network. Including this requirement as part of an organization's configuration standards and related processes ensures that only the necessary services and protocols are enabled.	YES				
	2.2.2.b Identify any enabled insecure services, daemons, or protocols and interview personnel to verify they are justified per documented configuration standards.						

2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure. *Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.*	2.2.3.a Inspect configuration settings to verify that security features are documented and implemented for all insecure services, daemons, or protocols. 2.2.3.b If SSL/early TLS is used, perform testing procedures in Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS.	Enabling security features before new servers are deployed will prevent servers being installed into the environment with insecure configurations. Ensuring that all insecure services, protocols, and daemons are adequately secured with appropriate security features makes it more difficult for malicious individuals to take advantage of commonly used points of compromise within a network.	YES				
2.2.4 Configure system security parameters to prevent misuse.	2.2.4.a Interview system administrators and/or security managers to verify that they have knowledge of common security parameter settings for system components. 2.2.4.b Examine the system configuration standards to verify that common security parameter settings are included. 2.2.4.c Select a sample of system components and inspect the common security parameters to verify that they are set appropriately and in accordance with the configuration standards.	System configuration standards and related processes should specifically address security settings and parameters that have known security implications for each type of system in use. In order for systems to be configured securely, personnel responsible for configuration and/or administering systems must be knowledgeable in the specific security parameters and settings that apply to the system.	YES				
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	2.2.5.a Select a sample of system components and inspect the configurations to verify that all unnecessary functionality (for example, scripts, drivers, features, subsystems, file systems, etc.) is removed. 2.2.5.b. Examine the documentation and security parameters to verify enabled functions are documented and support secure configuration. 2.2.5.c. Examine the documentation and security parameters to verify that only documented functionality is present on the sampled system components.	Unnecessary functions can provide additional opportunities for malicious individuals to gain access to a system. By removing unnecessary functionality, organizations can focus on securing the functions that are required and reduce the risk that unknown functions will be exploited. Including this in server-hardening standards and processes addresses the specific security implications associated with unnecessary functions (for example, by removing/disabling FTP or the web server if the server will not be performing those functions).	YES				
2.3 Encrypt all non-console administrative access using strong cryptography.	2.3 Select a sample of system components and verify that non-console administrative access is encrypted by performing the following: 2.3.a Observe an administrator log on to each system and examine system configurations to verify that a strong encryption method is invoked before the administrator's password is requested. 2.3.b Review services and parameter files on systems to determine that Telnet and other insecure remote-login commands are not available for non-console access. 2.3.c Observe an administrator log on to each system to verify that administrator access to any web-based management interfaces is encrypted with strong cryptography. 2.3.d Examine vendor documentation and interview personnel to verify that strong cryptography for the technology in use is implemented according to industry best practices and/or vendor recommendations. 2.3.e If SSL/early TLS is used, perform testing procedures in Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS.	If non-console (including remote) administration does not use secure authentication and encrypted communications, sensitive administrative or operational level information (like administrator's IDs and passwords) can be revealed to an eavesdropper. A malicious individual could use this information to access the network, become administrator, and steal data. Clear-text protocols (such as HTTP, telnet, etc.) do not encrypt traffic or logon details, making it easy for an eavesdropper to intercept this information. To be considered "strong cryptography," industry-recognized protocols with appropriate key strengths and key management should be in place as applicable for the type of technology in use. (Refer to "strong cryptography" in the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms, and industry standards and best practices such as NIST SP 800-52 and SP 800-57, OWASP, etc.)	YES				
2.4 Maintain an inventory of system components that are in scope for PCI DSS.	2.4.a Examine system inventory to verify that a list of hardware and software components is maintained and includes a description of function/use for each. 2.4.b Interview personnel to verify the documented inventory is kept current.	Maintaining a current list of all system components will enable an organization to accurately and efficiently define the scope of their environment for implementing PCI DSS controls. Without an inventory, some system components could be forgotten, and be inadvertently excluded from the organization's configuration standards.	YES				

2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	2.5 Examine documentation and interview personnel to verify that security policies and operational procedures for managing vendor defaults and other security parameters are: - Documented, - In use, and - Known to all affected parties.	Personnel need to be aware of and following security policies and daily operational procedures to ensure vendor defaults and other security parameters are continuously managed to prevent insecure configurations.	YES				
2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.	2.6 Perform testing procedures A.1.1 through A.1.4 detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers for PCI DSS assessments of shared hosting providers, to verify that shared hosting providers protect their entities' (merchants and service providers) hosted environment and data.	This is intended for hosting providers that provide shared hosting environments for multiple clients on the same server. When all data is on the same server and under control of a single environment, often the settings on these shared servers are not manageable by individual clients. This allows clients to add insecure functions and scripts that impact the security of all other client environments; and thereby make it easy for a malicious individual to compromise one client's data and thereby gain access to all other clients' data. See Appendix A for details of requirements.				YES	We are not a shared hosting provider, nor do we provid IT infrastructure as a service to our clients.

Requirement 3: Protect stored cardholder data

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should also be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.
Please refer to the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms for definitions of "strong cryptography" and other PCI DSS terms.

PCI DSS Control Details			Control Responsibility				Please provide additional details where the City of Vancouver's PCI Environment may be impacted.
PCI DSS Requirement	Testing Procedure	Guidance	100% Service Provider	100% City of Vancouver	Shared	N/A	
Requirement 3: Protect stored cardholder data							
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: - Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements - Processes for secure deletion of data when no longer needed - Specific retention requirements for cardholder data - A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.	3.1.a Examine the data retention and disposal policies, procedures and processes to verify they include at least the following: - Legal, regulatory, and business requirements for data retention, including - Specific requirements for retention of cardholder data (for example, cardholder data needs to be held for X period for Y business reasons). - Secure deletion of cardholder data when no longer needed for legal, regulatory, or business reasons - Coverage for all storage of cardholder data - A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements. 3.1.b Interview personnel to verify that: - All locations of stored cardholder data are included in the data retention and disposal processes. - Either a quarterly automatic or manual process is in place to identify and securely delete stored cardholder data. - The quarterly automatic or manual process is performed for all locations of cardholder data. 3.1.c For a sample of system components that store cardholder data: - Examine files and system records to verify that the data stored does not exceed the requirements defined in the data retention policy - Observe the deletion mechanism to verify data is deleted securely.	A formal data retention policy identifies what data needs to be retained, and where that data resides so it can be securely destroyed or deleted as soon as it is no longer needed. The only cardholder data that may be stored after authorization is the primary account number or PAN (rendered unreadable), expiration date, cardholder name, and service code. Understanding where cardholder data is located is necessary so it can be properly retained or disposed of when no longer needed. In order to define appropriate retention requirements, an entity first needs to understand their own business needs as well as any legal or regulatory obligations that apply to their industry, and/or that apply to the type of data being retained. Identifying and deleting stored data that has exceeded its specified retention period prevents unnecessary retention of data that is no longer needed. This process may be automated or manual or a combination of both. For example, a programmatic procedure (automatic or manual) to locate and remove data and/or a manual review of data storage areas could be performed. Implementing secure deletion methods ensure that the data cannot be retrieved when it is no longer needed. **Remember, if you don't need it, don't store it!**				YES	Cardholder data is securely transmitted directly to our 3rd party payment processors. The only derivitive data which we store are transation confirmation data which limits cardholder data to the last 4 digits of the card number. We store no other data.
3.2 Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process. *It is permissible for issuers and companies that support issuing services to store sensitive authentication data if:* *- There is a business justification and* *- The data is stored securely.* Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:	3.2.a For issuers and/or companies that support issuing services and store sensitive authentication data, review policies and interview personnel to verify there is a documented business justification for the storage of sensitive authentication data. 3.2.b For issuers and/or companies that support issuing services and store sensitive authentication data, examine data stores and system configurations to verify that the sensitive authentication data is secured. 3.2.c For all other entities, if sensitive authentication data is received, review policies and procedures, and examine system configurations to verify the data is not retained after authorization. 3.2.d For all other entities, if sensitive authentication data is received, review procedures and examine the processes for securely deleting the data to verify that the data is unrecoverable.	Sensitive authentication data consists of full track data, card validation code or value, and PIN data. Storage of sensitive authentication data after authorization is prohibited! This data is very valuable to malicious individuals as it allows them to generate counterfeit payment cards and create fraudulent transactions. Entities that issue payment cards or that perform or support issuing services will often create and control sensitive authentication data as part of the issuing function. It is allowable for companies that perform, facilitate, or support issuing services to store sensitive authentication data ONLY IF they have a legitimate business need to store such data. It should be noted that all PCI DSS requirements apply to issuers, and the only exception for issuers and issuer processors is that sensitive authentication data may be retained if there is a legitimate reason to do so. A legitimate reason is one that is necessary for the performance of the function being provided for the issuer and not one of convenience. Any such data must be stored securely and in accordance with all PCI DSS and specific payment brand requirements. For non-issuing entities, retaining sensitive authentication data post-authorization is not permitted.				YES	Our mobile app handles payment information and never transmits it to our servers. The card data is never stored in full on our servers, and only a reference key (a unique identifier string unrelated to the payment card itself) is stored on our servers which is used to reference the payment card data which is stored securely on our 3rd party payment processor. We never store the full payment card number on our servers. We never store the payment card expiration date on our servers. We never store the authorization code otherwise known as the 'CVV' code on the back of the card on our servers. We never store the PIN of the payment card on our servers.
3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere) after authorization. This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data. *Note: In the normal course of business, the following data elements from the magnetic stripe may need to be retained:* *- The cardholder's name* *- Primary account number (PAN)* *- Expiration date* *- Service code* *To minimize risk, store only these data elements as needed for business.*	3.2.1 For a sample of system components, examine data sources including but not limited to the following, and verify that the full contents of any track from the magnetic stripe on the back of card or equivalent data on a chip are not stored after authorization: - Incoming transaction data - All logs (for example, transaction, history, debugging, error) - History files - Trace files - Several database schemas - Database contents.	If full track data is stored, malicious individuals who obtain that data can use it to reproduce payment cards and complete fraudulent transactions.				YES	Our mobile app handles payment information and never transmits it to our servers. Moreover, mobile app receives card data from manual entry by the user and not via magnetic swipe or via chipreader.

3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions after authorization.	3.2.2 For a sample of system components, examine data sources, including but not limited to the following, and verify that the three-digit or four-digit card verification code or value printed on the front of the card or the signature panel (CVV2, CVC2, CID, CAV2 data) is not stored after authorization: - Incoming transaction data - All logs (for example, transaction, history, debugging, error) - History files - Trace files - Several database schemas - Database contents.	The purpose of the card validation code is to protect "card-not-present" transactions—Internet or mail order/telephone order (MO/TO) transactions—where the consumer and the card are not present. If this data is stolen, malicious individuals can execute fraudulent Internet and MO/TO transactions.				YES	Our mobile app handles payment information and never transmits it to our servers. The card data is never stored in full on our servers, and only a reference key (a unique identifier string unrelated to the payment card itself) is stored on our servers which is used to reference the payment card data which is stored securely on our 3rd party payment processor. We never store the full payment card number on our servers. We never store the payment card expiration date on our servers. We never store the authorization code otherwise known as the 'CVV' code on the back of the card on our servers. We never store the PIN of the payment card on our servers.
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.	3.2.3 For a sample of system components, examine data sources, including but not limited to the following and verify that PINs and encrypted PIN blocks are not stored after authorization: - Incoming transaction data - All logs (for example, transaction, history, debugging, error) - History files - Trace files - Several database schemas - Database contents.	These values should be known only to the card owner or bank that issued the card. If this data is stolen, malicious individuals can execute fraudulent PIN-based debit transactions (for example, ATM withdrawals).				YES	Our mobile app handles payment information and never transmits it to our servers. The card data is never stored in full on our servers, and only a reference key (a unique identifier string unrelated to the payment card itself) is stored on our servers which is used to reference the payment card data which is stored securely on our 3rd party payment processor. We never store the full payment card number on our servers. We never store the payment card expiration date on our servers. We never store the authorization code otherwise known as the 'CVV' code on the back of the card on our servers. We never store the PIN of the payment card on our servers.
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN. *Note: This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.*	3.3.a Examine written policies and procedures for masking the display of PANs to verify: - A list of roles that need access to displays of full PAN is documented, together with a legitimate business need for each role to have such access. - PAN must be masked when displayed such that only personnel with a legitimate business need can see the full PAN. - All other roles not specifically authorized to see the full PAN must only see masked PANs. 3.3.b Examine system configurations to verify that full PAN is only displayed for users/roles with a documented business need, and that PAN is masked for all other requests. 3.3.c Examine displays of PAN (for example, on screen, on paper receipts) to verify that PANs are masked when displaying cardholder data, and that only those with a legitimate business need are able to see full PAN.	The display of full PAN on items such as computer screens, payment card receipts, faxes, or paper reports can result in this data being obtained by unauthorized individuals and used fraudulently. Ensuring that full PAN is only displayed for those with a legitimate business need to see the full PAN minimizes the risk of unauthorized persons gaining access to PAN data. This requirement relates to protection of PAN displayed on screens, paper receipts, printouts, etc., and is not to be confused with Requirement 3.4 for protection of PAN when stored in files, databases, etc.				YES	The card data is never stored in full on our servers, and only a reference key (a unique identifier string unrelated to the payment card itself) is stored on our servers which is used to reference the payment card data which is stored securely on our 3rd party payment processor. We never store the full payment card number on our servers. We never store the payment card expiration date on our servers. We never store the authorization code otherwise known as the 'CVV' code on the back of the card on our servers. We never store the PIN of the payment card on our servers. Only the last 4 digits of the PAN are stored for display purposes, these are provided to us by the payment processor.
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: - One-way hashes based on strong cryptography, (hash must be of the entire PAN) - Truncation (hashing cannot be used to replace the truncated segment of PAN) - Index tokens and pads (pads must be securely stored) - Strong cryptography with associated key-management processes and procedures. *Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls must be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN .*	3.4.a Examine documentation about the system used to protect the PAN, including the vendor, type of system/process, and the encryption algorithms (if applicable) to verify that the PAN is rendered unreadable using any of the following methods: - One-way hashes based on strong cryptography, - Truncation - Index tokens and pads, with the pads being securely stored - Strong cryptography, with associated key-management processes and procedures. 3.4.b Examine several tables or files from a sample of data repositories to verify the PAN is rendered unreadable (that is, not stored in plain-text). 3.4.c Examine a sample of removable media (for example, back-up tapes) to confirm that the PAN is rendered unreadable. 3.4.d Examine a sample of audit logs to confirm that the PAN is rendered unreadable or removed from the logs. 3.4.e If hashed and truncated versions of the same PAN are present in the environment, examine implemented controls to verify that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.	PANs stored in primary storage (databases, or flat files such as text files spreadsheets) as well as non-primary storage (backup, audit logs, exception or troubleshooting logs) must all be protected. One-way hash functions based on strong cryptography can be used to render cardholder data unreadable. Hash functions are appropriate when there is no need to retrieve the original number (one-way hashes are irreversible). It is recommended, but not currently a requirement, that an additional, random input value be added to the cardholder data prior to hashing to reduce the feasibility of an attacker comparing the data against (and deriving the PAN from) tables of pre-computed hash values. The intent of truncation is to permanently remove a segment of PAN data so that only a portion (generally not to exceed the first six and last four digits) of the PAN is stored. An index token is a cryptographic token that replaces the PAN based on a given index for an unpredictable value. A one-time pad is a system in which a randomly generated private key is used only once to encrypt a message that is then decrypted using a matching one-time pad and key. The intent of strong cryptography (as defined in the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms) is that the encryption be based on an industry-tested and accepted algorithm (not a proprietary or "home-grown" algorithm) with strong cryptographic keys. By correlating hashed and truncated versions of a given PAN, a malicious individual may easily derive the original PAN value. Controls that prevent the correlation of this data will help ensure that the original PAN remains unreadable.				YES	The card data is never stored in full on our servers, and only a reference key (a unique identifier string unrelated to the payment card itself) is stored on our servers which is used to reference the payment card data which is stored securely on our 3rd party payment processor. We never store the full payment card number on our servers. We never store the payment card expiration date on our servers. We never store the authorization code otherwise known as the 'CVV' code on the back of the card on our servers. We never store the PIN of the payment card on our servers. Only the last 4 digits of the PAN are stored for display purposes, these are provided to us by the payment processor.
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts. *Note: This requirement applies in addition to all other PCI*	3.4.1.a If disk encryption is used, inspect the configuration and observe the authentication process to verify that logical access to encrypted file systems is implemented via a mechanism that is separate from the native operating system's authentication mechanism (for example, not using local user account databases or general network login credentials). 3.4.1.b Observe processes and interview personnel to verify that cryptographic keys are stored securely (for example, stored on removable media that is adequately protected with strong access controls).	The intent of this requirement is to address the acceptability of disk-level encryption for rendering cardholder data unreadable. Disk-level encryption encrypts the entire disk/partition on a computer and automatically decrypts the information when an authorized user requests it. Many disk-encryption solutions intercept operating system read/write operations and carry out the appropriate cryptographic transformations without any special action by the user other than supplying a password or pass phrase upon system startup or at the beginning of a session. Based on these characteristics of disk-level encryption, to be compliant with this requirement, the method cannot: 1) Use the same user account authenticator as the operating system, or	YES				

DSS encryption and key-management requirements.	3.4.1.c Examine the configurations and observe the processes to verify that cardholder data on removable media is encrypted wherever stored. *Note: If disk encryption is not used to encrypt removable media, the data stored on this media will need to be rendered unreadable through some other method.*	2) Use a decryption key that is associated with or derived from the system's local user account database or general network login credentials. Full disk encryption helps to protect data in the event of physical loss of a disk and therefore may be appropriate for portable devices that store cardholder data.					
3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse: *Note: This requirement applies to keys used to encrypt stored cardholder data, and also applies to key-encrypting keys used to protect data-encrypting keys—such key-encrypting keys must be at least as strong as the data-encrypting key.*	3.5 Examine key-management policies and procedures to verify processes are specified to protect keys used for encryption of cardholder data against disclosure and misuse and include at least the following: - Access to keys is restricted to the fewest number of custodians necessary. - Key-encrypting keys are at least as strong as the data-encrypting keys they protect. - Key-encrypting keys are stored separately from data-encrypting keys. - Keys are stored securely in the fewest possible locations and forms.	Cryptographic keys must be strongly protected because those who obtain access will be able to decrypt data. Key-encrypting keys, if used, must be at least as strong as the data-encrypting key in order to ensure proper protection of the key that encrypts the data as well as the data encrypted with that key. The requirement to protect keys from disclosure and misuse applies to both data-encrypting keys and key-encrypting keys. Because one key-encrypting key may grant access to many data-encrypting keys, the key-encrypting keys require strong protection measures.				YES	The card data is never stored in full on our servers, and only a reference key (a unique identifier string unrelated to the payment card itself) is stored on our servers which is used to reference the payment card data which is stored securely on our 3rd party payment processor. We never store the full payment card number on our servers. We never store the payment card expiration date on our servers. We never store the authorization code otherwise known as the 'CVV' code on the back of the card on our servers. We never store the PIN of the payment card on our servers. Only the last 4 digits of the PAN are stored for display purposes, these are provided to us by the payment processor.
3.5.1 Additional requirement for service providers only: Maintain a documented description of the cryptographic architecture that includes: - Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date - Description of the key usage for each key - Inventory of any HSMs and other SCDs used for key management *Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*	3.5.1 Interview responsible personnel and reviewdocumentation to verify that a document exists to describe the cryptographic architecture, including: - Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date - Description of the key usage for each key - Inventory of any HSMs and other SCDs used for key management	Note: This requirement applies only when the entity being assessed is a service provider. Maintaining current documentation of the cryptographic architecture enables an entity to understand the algorithms, protocols, and cryptographic keys used to protect cardholder data, as well as the devices that generate, use and protect the keys. This allows an entity to keep pace with evolving threats to their architecture, enabling them to plan for updates as the assurance levels provided by different algorithms/key strengths changes. Maintaining such documentation also allows an entity to detect lost or missing keys or key-management devices, and identify unauthorized additions to their cryptographic architecture.				YES	We do not store any full or usable cardholder data, including expiration dates, CVV codes, PINS, and PANs.
3.5.2 Restrict access to cryptographic keys to the fewest number of custodians necessary.	3.5.2 Examine user access lists to verify that access to keys is restricted to the fewest number of custodians necessary.	There should be very few who have access to cryptographic keys reducing the potential for rending cardholder data visible by unauthorized parties), usually only those who have key custodian responsibilities.				YES	We do not store any full or usable cardholder data, including expiration dates, CVV codes, PINS, and PANs.
3.5.3 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times: - Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key - Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) - As at least two full-length key components or key shares, in accordance with an industry- accepted method *Note: It is not required that public keys be stored in one of these forms.*	3.5.3.a Examine documented procedures to verify that cryptographic keys used to encrypt/decrypt cardholder data must only exist in one (or more) of the following forms at all times. - Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key - Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) - As key components or key shares, in accordance with an industry-accepted method	Cryptographic keys must be stored securely to prevent unauthorized or unnecessary access that could result in the exposure of cardholder data. It is not intended that the key-encrypting keys be encrypted, however they are to be protected against disclosure and misuse as defined in Requirement 3.5. If key-encrypting keys are used, storing the key-encrypting keys in physically and/or logically separate locations from the data-encrypting keys reduces the risk of unauthorized access to both keys.				YES	The card data is never stored in full on our servers, and only a reference key (a unique identifier string unrelated to the payment card itself) is stored on our servers which is used to reference the payment card data which is stored securely on our 3rd party payment processor. We never store the full payment card number on our servers. We never store the payment card expiration date on our servers. We never store the authorization code otherwise known as the 'CVV' code on the back of the card on our servers. We never store the PIN of the payment card on our servers. Only the last 4 digits of the PAN are stored for display purposes, these are provided to us by the payment processor.
	3.5.3.b Examine system configurations and key storage locations to verify that cryptographic keys used to encrypt/decrypt cardholder data exist in one (or more) of the following form at all times. • Encrypted with a key-encrypting key • Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device) • As key components or key shares, in accordance with an industry-accepted method						
	3.5.3.c Wherever key-encrypting keys are used, examine system configurations and key storage locations to verify: - Key-encrypting keys are at least as strong as the data- encrypting keys they protect - Key-encrypting keys are stored separately from data-encrypting keys.						
3.5.4 Store cryptographic keys in the fewest possible locations	3.5.4 Examine key storage locations and observe processes to verify that keys are stored in the fewest possible locations.	Storing cryptographic keys in the fewest locations helps an organization to keep track and monitor all key locations, and minimizes the potential for keys to be exposed to unauthorized parties.				YES	We do not store any full or usable cardholder data, including expiration dates, CVV codes, PINS, and PANs.

3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: *Note: Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.*	3.6.a ***Additional testing procedure for service provider assessments only:*** If the service provider shares keys with their customers for transmission or storage of cardholder data, examine the documentation that the service provider provides to their customers to verify that it includes guidance on how to securely transmit, store, and update customers' keys, in accordance with Requirements 3.6.1 through 3.6.8 below. 3.6.b Examine the key-management procedures and processes for keys used for encryption of cardholder data and perform the following:	The manner in which cryptographic keys are managed is a critical part of the continued security of the encryption solution. A good key-management process, whether it is manual or automated as part of the encryption product, is based on industry standards and addresses all key elements at 3.6.1 through 3.6.8. Providing guidance to customers on how to securely transmit, store and update cryptographic keys can help prevent keys from being mismanaged or disclosed to unauthorized entities. This requirement applies to keys used to encrypt stored cardholder data, and any respective key-encrypting keys.				YES	The card data is never stored in full on our servers, and only a reference key (a unique identifier string unrelated to the payment card itself) is stored on our servers which is used to reference the payment card data which is stored securely on our 3rd party payment processor. We never store the full payment card number on our servers. We never store the payment card expiration date on our servers. We never store the authorization code otherwise known as the 'CVV' code on the back of the card on our servers. We never store the PIN of the payment card on our servers. Only the last 4 digits of the PAN are stored for display purposes, these are provided to us by the payment processor.
3.6.1 Generation of strong cryptographic keys	3.6.1.a Verify that key-management procedures specify how to generate strong keys. 3.6.1.b Observe the method for generating keys to verify that strong keys are generated.	The encryption solution must generate strong keys, as defined in the PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms under "strong cryptography." Use of strong cryptographic keys significantly increases the level of security of encrypted cardholder data.				YES	We do not store any full or usable cardholder data, including expiration dates, CVV codes, PINS, and PANs.
3.6.2 Secure cryptographic key distribution	3.6.2.a Verify that key-management procedures specify how to securely distribute keys. 3.6.2.b Observe the method for distributing keys to verify that keys are distributed securely.	The encryption solution must distribute keys securely, meaning the keys are distributed only to custodians identified in 3.5.1, and are never distributed in the clear.				YES	We do not store any full or usable cardholder data, including expiration dates, CVV codes, PINS, and PANs.
3.6.3 Secure cryptographic key storage	3.6.3.a Verify that key-management procedures specify how to securely store keys. 3.6.3.b Observe the method for storing keys to verify that keys are stored securely.	The encryption solution must store keys securely, for example, by encrypting them with a key-encrypting key. Storing keys without proper protection could provide access to attackers, resulting in the decryption and exposure of cardholder data.				YES	We do not store any full or usable cardholder data, including expiration dates, CVV codes, PINS, and PANs.
3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).	3.6.4.a Verify that key-management procedures include a defined cryptoperiod for each key type in use and define a process for key changes at the end of the defined cryptoperiod(s). 3.6.4.b Interview personnel to verify that keys are changed at the end of the defined cryptoperiod(s).	A cryptoperiod is the time span during which a particular cryptographic key can be used for its defined purpose. Considerations for defining the cryptoperiod include, but are not limited to, the strength of the underlying algorithm, size or length of the key, risk of key compromise, and the sensitivity of the data being encrypted. Periodic changing of encryption keys when the keys have reached the end of their cryptoperiod is imperative to minimize the risk of someone's obtaining the encryption keys, and using them to decrypt data.				YES	We do not store any full or usable cardholder data, including expiration dates, CVV codes, PINS, and PANs.
3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised. *Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key-encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.*	3.6.5.a Verify that key-management procedures specify processes for the following: - The retirement or replacement of keys when the integrity of the key has been weakened - The replacement of known or suspected compromised keys. - Any keys retained after retiring or replacing are not used for encryption operations 3.6.5.b Interview personnel to verify the following processes are implemented: - Keys are retired or replaced as necessary when the integrity of the key has been weakened, including when someone with knowledge of the key leaves the company. - Keys are replaced if known or suspected to be compromised. - Any keys retained after retiring or replacing are not used for encryption operations.	Keys that are no longer used or needed, or keys that are known or suspected to be compromised, should be revoked and/or destroyed to ensure that the keys can no longer be used. If such keys need to be kept (for example, to support archived, encrypted data) they should be strongly protected. The encryption solution should provide for and facilitate a process to replace keys that are due for replacement or that are known to be, or suspected of being, compromised.				YES	We do not store any full or usable cardholder data, including expiration dates, CVV codes, PINS, and PANs.
3.6.6 If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control. *Note: Examples of manual key-management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.*	3.6.6.a Verify that manual clear-text key-management procedures specify processes for the use of the following: - Split knowledge of keys, such that key components are under the control of at least two people who only have knowledge of their own key components; AND - Dual control of keys, such that at least two people are required to perform any key-management operations and no one person has access to the authentication materials (for example, passwords or keys) of another. 3.6.6 b Interview personnel and/or observe processes to verify that manual clear-text keys are managed with: - Split knowledge, AND - Dual control	Split knowledge and dual control of keys are used to eliminate the possibility of one person having access to the whole key. This control is applicable for manual key-management operations, or where key management is not implemented by the encryption product. Split knowledge is a method in which two or more people separately have key components, where each person knows only their own key component, and the individual key components convey no knowledge of the original cryptographic key). Dual control requires two or more people to perform a function, and no single person can access or use the authentication materials of another.				YES	We do not store any full or usable cardholder data, including expiration dates, CVV codes, PINS, and PANs.
3.6.7 Prevention of unauthorized substitution of cryptographic keys.	3.6.7.a Verify that key-management procedures specify processes to prevent unauthorized substitution of keys. 3.6.7.b Interview personnel and/or observe processes to verify that unauthorized substitution of keys is prevented.	The encryption solution should not allow for or accept substitution of keys coming from unauthorized sources or unexpected processes.				YES	We do not store any full or usable cardholder data, including expiration dates, CVV codes, PINS, and PANs.
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	3.6.8.a Verify that key-management procedures specify processes for key custodians to acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.	This process will help ensure individuals that act as key custodians commit to the key-custodian role and understand and accept the responsibilities.				YES	We do not store any full or usable cardholder data, including expiration

	3.6.8.b Observe documentation or other evidence showing that key custodians have acknowledged (in writing or electronically) that they understand and accept their key-custodian responsibilities.					YES	dates, CVV codes, PINS, and PANs.
3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.	3.7 Examine documentation interview personnel to verify that security policies and operational procedures for protecting stored cardholder data are: - Documented, - In use, and - Known to all affected parties.	Personnel need to be aware of and following security policies and documented operational procedures for managing the secure storage of cardholder data on a continuous basis.				YES	We do not store any full or usable cardholder data, including expiration dates, CVV codes, PINS, and PANs.

Requirement 4: Encrypt transmission of cardholder data across open, public networks
Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments

PCI DSS Control Details			Control Responsibility				
PCI DSS Requirement	**Testing Procedure**	**Guidance**	**100% Service Provider**	**100% City of Vancouver**	**Shared**	**N/A**	**Please provide additional details where the City of Vancouver's PCI Environment may be impacted.**
Requirement 4: Encrypt transmission of cardholder data across open, public networks							
4.1 Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following: - Only trusted keys and certificates are accepted. - The protocol in use only supports secure versions or configurations. - The encryption strength is appropriate for the encryption methodology in use. *Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.* *Examples of open, public networks include but are not limited to:* *- The Internet* *- Wireless technologies, including 802.11 and Bluetooth* *- Cellular technologies, for example, Global System for Mobile communications (GSM), Code division multiple access (CDMA)* *- General Packet Radio Service (GPRS)* *- Satellite communications*	4.1.a Identify all locations where cardholder data is transmitted or received over open, public networks. Examine documented standards and compare to systemconfigurations to verify the use of security protocols and strong cryptography for all locations. 4.1.b Review documented policies and procedures to verify processes are specified for the following: - For acceptance of only trusted keys and/or certificates - For the protocol in use to only support secure versions and configurations (that insecure versions or configurations are not supported) - For implementation of proper encryption strength per the encryption methodology in use 4.1.c Select and observe a sample of inbound and outbound transmissions as they occur to verify that all cardholder data is encrypted with strong cryptography during transit. 4.1.d Examine keys and certificates to verify that only trusted keys and/or certificates are accepted. 4.1.e Examine system configurations to verify that the protocol is implemented to use only secure configurations and does not support insecure versions or configurations. 4.1.f Examine system configurations to verify that the proper encryption strength is implemented for the encryption methodology in use. (Check vendor recommendations/best practices.) 4.1.g For TLS implementations, examine system configurations to verify that TLS is enabled whenever cardholder data is transmitted or received. For example, for browser-based implementations: • "HTTPS" appears as the browser Universal Record Locator (URL) protocol; and • Cardholder data is only requested if "HTTPS" appears as part of the URL. 4.1.h If SSL/early TLS is used, perform testing procedures in Appendix A2: Additional PCI DSS Requirements for Entities using SSL/Early TLS.	Sensitive information must be encrypted during transmission over public networks, because it is easy and common for a malicious individual to intercept and/or divert data while in transit. Secure transmission of cardholder data requires using trusted keys/certificates, a secure protocol for transport, and proper encryption strength to encrypt cardholder data. Connection requests from systems that do not support the required encryption strength, and that would result in an insecure connection, should not be accepted. Note that some protocol implementations (such as SSL, SSH v1.0, and early TLS) have known vulnerabilities that an attacker can use to gain control of the affected system. Whichever security protocol is used, ensure it is configured to use only secure versions and configurations to prevent use of an insecure connection—for example, by using only trusted certificates and supporting only strong encryption (not supporting weaker, insecure protocols or methods). Verifying that certificates are trusted (for example, have not expired and are issued from a trusted source) helps ensure the integrity of the secure connection. Generally, the web page URL should begin with "HTTPS" and/or the web browser display a padlock icon somewhere in the window of the browser. Many TLS certificate vendors also provide a highly visible verification seal—sometimes referred to as a "security seal," "secure site seal," or "secure trust seal")—which may provide the ability to click on the seal to reveal information about the website. Refer to industry standards and best practices for information on strong cryptography and secure protocols (e.g., NIST SP 800-52 and SP 800-57, OWASP, etc.)	YES				**Example:** Customers are responsible for ensuring strong cryptography and secure protocols are used to connect to their [Name of Third Party Service]environment.
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.	4.1.1 Identify all wireless networks transmitting cardholder data or connected to the cardholder data environment. Examine documented standards and compare to system configuration settings to verify the following for all wireless networks identified: - Industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission. - Weak encryption (for example, WEP, SSL) is not used as a security control for authentication or transmission.	Malicious users use free and widely available tools to eavesdrop on wireless communications. Use of strong cryptography can help limit disclosure of sensitive information across wireless networks. Strong cryptography for authentication and transmission of cardholder data is required to prevent malicious users from gaining access to the wireless network or utilizing wireless networks to access other internal networks or data.				YES	Payment processing happen from our mobile app via our 3rd party payment processor SDKs, and we do not control the networks from which the mobile devices that send these transmissions.
4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).	4.2.a If end-user messaging technologies are used to send cardholder data, observe processes for sending PAN and examine a sample of outbound transmissions as they occur to verify that PAN is rendered unreadable or secured with strong cryptography whenever it is sent via end-user messaging technologies. 4.2.b Review written policies to verify the existence of a policy stating that unprotected PANs are not to be sent via end-user messaging technologies.	E-mail, instant messaging, SMS, and chat can be easily intercepted by packet-sniffing during delivery across internal and public networks. Do not utilize these messaging tools to send PAN unless they are configured to provide strong encryption. Additionally, if an entity requests PAN via end-user messaging technologies, the entity should provide a tool or method to protect these PANs using strong cryptography or render PANs unreadable before transmission.				YES	We never transmit PAN (personal payment card account numbers) over messaging applications or email. Our 3rd party payment processing provider, utilizes an SDK which our developers integrate into our mobile app. This SDK encrypts the payment data prior to transmission.
4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.	4.3 Examine documentation interview personnel to verify that security policies and operational procedures for encrypting transmissions of cardholder data are: - Documented, - In use, and - Known to all affected parties.	Personnel need to be aware of and following security policies and operational procedures for managing the secure transmission of cardholder data on a continuous basis.	YES				

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

Malicious software, commonly referred to as "malware"—including viruses, worms, and Trojans—enters the network during many business-approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats. Additional anti-malware solutions may be considered as a supplement to the anti-virus software; however, such additional solutions do not replace the need for anti-virus software to be in place.

PCI DSS Control Details			Control Responsibility				
PCI DSS Requirement	**Testing Procedure**	**Guidance**	**100% Service Provider**	**100% City of Vancouver**	**Shared**	**N/A**	**Please provide additional details where the City of Vancouver's PCI Environment may be impacted.**
Requirement 5: Use and regularly update anti-virus software or programs							
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	5.1 For a sample of system components including all operating system types commonly affected by malicious software, verify that anti-virus software is deployed if applicable anti-virus technology exists.	There is a constant stream of attacks using widely published exploits, often called "zero day" (an attack that exploits a previously unknown vulnerability), against otherwise secured systems. Without an anti-virus solution that is updated regularly, these new forms of malicious software can attack systems, disable a network, or lead to compromise of data.	YES				**Example:** Customers are responsible for ensuring anti-malware software is deployed on all systems in the CDE commonly affected by malicious software. Customers may enable [Name of Third Party Service] Antimalware to leverage [Name of Service Provider] anti-malware protections. Customers are still responsibe for configuration options under their control.
5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	5.1.1 Review vendor documentation and examine anti-virus configurations to verify that anti-virus programs; - Detect all known types of malicious software, - Remove all known types of malicious software, and - Protect against all known types of malicious software. *Examples of types of malicious software include viruses, Trojans, worms, spyware, adware, and rootkits.*	It is important to protect against ALL types and forms of malicious software.	YES				
5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.	5.1.2 Interview personnel to verify that evolving malware threats are monitored and evaluated for systems not currently considered to be commonly affected by malicious software, in order to confirm whether such systems continue to not require anti-virus software.	Typically, mainframes, mid-range computers (such as AS/400) and similar systems may not currently be commonly targeted or affected by malware. However, industry trends for malicious software can change quickly, so it is important for organizations to be aware of new malware that might affect their systems—for example, by monitoring vendor security notices and anti-virus news groups to determine whether their systems might be coming under threat from new and evolving malware. Trends in malicious software should be included in the identification of new security vulnerabilities, and methods to address new trends should be incorporated into the company's configuration standards and protection mechanisms as needed	YES				
5.2 Ensure that all anti-virus mechanisms are maintained as follows: - Are kept current, - Perform periodic scans - Generate audit logs which are retained per PCI DSS Requirement 10.7.	5.2.a Examine policies and procedures to verify that anti-virus software and definitions are required to be kept up to date. 5.2.b Examine anti-virus configurations, including the master installation of the software to verify anti-virus mechanisms are: - Configured to perform automatic updates, and - Configured to perform periodic scans. 5.2.c Examine a sample of system components, including all operating system types commonly affected by malicious software, to verify that: - The anti-virus software and definitions are current. - Periodic scans are performed. 5.2.d Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that: - Anti-virus software log generation is enabled, and - Logs are retained in accordance with PCI DSS Requirement 10.7.	Even the best anti-virus solutions are limited in effectiveness if they are not maintained and kept current with the latest security updates, signature files, or malware protections. Audit logs provide the ability to monitor virus and malware activity and anti-malware reactions. Thus, it is imperative that anti-malware solutions be configured to generate audit logs and that these logs be managed in accordance with Requirement 10.	YES				
5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized	5.3.a Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify the anti-virus software is actively running.	Anti-virus that continually runs and is unable to be altered will provide persistent security against malware. Use of policy-based controls on all systems to ensure anti-malware					

by management on a case-by-case basis for a limited time period. *Note: Anti-virus solutions may be temporarily disabled only if there is legitimate technical need, as authorized by management on a case-by-case basis. If anti-virus protection needs to be disabled for a specific purpose, it must be*	5.3.b Examine anti-virus configurations, including the master installation of the software and a sample of system components, to verify that the anti-virus software cannot be disabled or altered by 5.3.c Interview responsible personnel and observe processes to verify that anti-virus software cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	protections cannot be altered or disabled will help prevent system weaknesses from being exploited by malicious software. Additional security measures may also need to be implemented for the period of time during which anti-virus protection is not active—for example, disconnecting the unprotected system from the Internet while the anti-virus protection is disabled, and running a full scan after it is re-enabled.	YES				
5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	5.4 Examine documentation and interview personnel to verify that security policies and operational procedures for protecting systems against malware are: - Documented, - In use, and - Known to all affected parties.	Personnel need to be aware of and following security policies and operational procedures to ensure systems are protected from malware on a continuous basis.	YES				

Requirement 6: Develop and maintain secure systems and applications

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All systems must have all appropriate software patches to protect against the exploitation and compromise of cardholder data by malicious individuals and malicious software. Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.

PCI DSS Control Details			Control Responsibility				
PCI DSS Requirement	**Testing Procedure**	**Guidance**	**100% Service Provider**	**100% City of Vancouver**	**Shared**	**N/A**	**Please provide additional details where the City of Vancouver's PCI Environment may be impacted.**
Requirement 6: Develop and maintain secure sysetms and applications							
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities. *Note: Risk rankings should be based on industry best practices as well as consideration of potential impact. For example, criteria for ranking vulnerabilities may include consideration of the CVSS base score, and/or the classification by the vendor, and/or type of systems affected. Methods for evaluating vulnerabilities and assigning risk ratings will vary based on an organization's environment and risk-assessment strategy. Risk rankings should, at a minimum, identify all vulnerabilities considered to be a "high risk" to the environment. In addition to the risk ranking, vulnerabilities may be considered "critical" if they pose an imminent threat to the environment, impact critical systems, and/or would result in a potential compromise if not addressed. Examples of critical systems may include security systems, public-facing devices and systems, databases, and other systems that store, process, or transmit cardholder data.*	6.1.a Examine policies and procedures to verify that processes are defined for the following: - To identify new security vulnerabilities - To assign a risk ranking to vulnerabilities that includes identification of all "high risk" and "critical" vulnerabilities. - To use reputable outside sources for security vulnerability information.	The intent of this requirement is that organizations keep up to date with new vulnerabilities that may impact their environment. Sources for vulnerability information should be trustworthy and often include vendor websites, industry news groups, mailing list, or RSS feeds. Once an organization identifies a vulnerability that could affect their environment, the risk that the vulnerability poses must be evaluated and ranked. The organization must therefore have a method in place to evaluate vulnerabilities on an ongoing basis and assign risk rankings to those vulnerabilities. This is not achieved by an ASV scan or internal vulnerability scan, rather this requires a process to actively monitor industry sources for vulnerability information. Classifying the risks (for example, as "high," "medium," or "low") allows organizations to identify, prioritize, and address the highest risk items more quickly and reduce the likelihood that vulnerabilities posing the greatest risk will be exploited.	YES				
	6.1.b Interview responsible personnel and observe processes to verify that: - New security vulnerabilities are identified. - A risk ranking is assigned to vulnerabilities that includes identification of all "high" risk and "critical" vulnerabilities. - Processes to identify new security vulnerabilities include using reputable outside sources for security vulnerability information.						
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release. *Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1.*	6.2.a Examine policies and procedures related to security-patch installation to verify processes are defined for: - Installation of applicable critical vendor-supplied security patches within one month of release. - Installation of all applicable vendor-supplied security patches within an appropriate time frame (for example, within three months).	There is a constant stream of attacks using widely published exploits, often called "zero day" (an attack that exploits a previously unknown vulnerability), against otherwise secured systems. If the most recent patches are not implemented on critical systems as soon as possible, a malicious individual can use these exploits to attack or disable a system, or gain access to sensitive data. Prioritizing patches for critical infrastructure ensures that high-priority systems and devices are protected from vulnerabilities as soon as possible after a patch is released. Consider prioritizing patch installations such that security patches for critical or at-risk systems are installed within 30 days, and other lower-risk patches are installed within 2-3 months. This requirement applies to applicable patches for all installed software, including payment applications (both those that are PA-DSS validated and thosethat are not).	YES				
	6.2.b For a sample of system components and related software, compare the list of security patches installed on each system to the most recent vendor security-patch list, to verify the following: - That applicable critical vendor-supplied security patches are installed within one month of release. - All applicable vendor-supplied security patches are installed within an appropriate time frame (for example, within three months).						
6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: - In accordance with PCI DSS (for example, secure authentication and logging) - Based on industry standards and/or best practices. - Incorporating information security throughout the software-development life cycle Note: this applies to all software developed internally as well as bespoke or custom software developed by a	6.3.a Examine written software-development processes to verify that the processes are based on industry standards and/or best practices.	Without the inclusion of security during the requirements definition, design, analysis, and testing phases of software development, security vulnerabilities can be inadvertently or maliciously introduced into the production environment. Understanding how sensitive data is handled by the application—including when stored, transmitted, and when in memory—can help identify where data needs to be protected.	YES				
	6.3.b Examine written software-development processes to verify that information security is included throughout the life cycle.						
	6.3.c Examine written software-development processes to verify that software applications are developed in accordance with PCI DSS.						
	6.3.d Interview software developers to verify that written software-development processes are implemented.						

6.3.1 Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	6.3.1 Examine written software-development procedures and interview responsible personnel to verify that pre-production and/or custom application accounts, user IDs and/or passwords are removed before an application goes into production or is released to customers.	Development, test and/or custom application accounts, user IDs, and passwords should be removed from production code before the application becomes active or is released to customers, since these items may give away information about the functioning of the application. Possession of such information could facilitate compromise of the application and related cardholder data.	YES				
6.3.2 Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following: - Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices. - Code reviews ensure code is developed according to secure coding guidelines - Appropriate corrections are implemented prior to release. - Code-review results are reviewed and approved by management prior to release. *Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle. Code reviews can be conducted by knowledgeable internal personnel or third parties. Public-facing web applications are also subject to additional controls, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.*	6.3.2.a Examine written software-development procedures and interview responsible personnel to verify that all custom application code changes must be reviewed (using either manual or automated processes) as follows: - Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code-review techniques and secure coding practices. - Code reviews ensure code is developed according to secure coding guidelines (see PCI DSS Requirement 6.5). - Appropriate corrections are implemented prior to release. - Code-review results are reviewed and approved by management prior to release. 6.3.2.b Select a sample of recent custom application changes and verify that custom application code is reviewed according to 6.3.2.a, above.	Security vulnerabilities in custom code are commonly exploited by malicious individuals to gain access to a network and compromise cardholder data. An individual knowledgeable and experienced in code-review techniques should be involved in the review process. Code reviews should be performed by someone other than the developer of the code to allow for an independent, objective review. Automated tools or processes may also be used in lieu of manual reviews, but keep in mind that it may be difficult or even impossible for an automated tool to identify some coding issues. Correcting coding errors before the code is deployed into a production environment or released to customers prevents the code exposing the environments to potential exploit. Faulty code is also far more difficult and expensive to address after it has been deployed or released into production environments. Including a formal review and signoff by management prior to release helps to ensure that code is approved and has been developed in accordance with policies and procedures.	YES				
6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:	6.4 Examine policies and procedures to verify the following are defined: - Development/test environments are separate from production environments with access control in place to enforce separation. - A separation of duties between personnel assigned to the development/test environments and those assigned to the production environment. - Production data (live PANs) are not used for testing or development. - Test data and accounts are removed before a production system becomes active. - Change control procedures related to implementing security patches and software modifications are documented.	Without properly documented and implemented change controls, security features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur, or malicious code could be introduced.	YES				
6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls.	6.4.1.a Examine network documentation and network device configurations to verify that the development/test environments are separate from the production environment(s). 6.4.1.b Examine access controls settings to verify that access controls are in place to enforce separation between the development/test environments and the production environment(s).	Due to the constantly changing state of development and test environments, they tend to be less secure than the production environment. Without adequate separation between environments, it may be possible for the production environment, and cardholder data, to be compromised due to less-stringent security configurations and possible vulnerabilities in a test or development environment.	YES				
6.4.2 Separation of duties between development/test and production environments	6.4.2 Observe processes and interview personnel assigned to development/test environments and personnel assigned to production environments to verify that separation of duties is in place between development/test environments and the production environment.	Reducing the number of personnel with access to the production environment and cardholder data minimizes risk and helps ensure that access is limited to those individuals with a business need to know. The intent of this requirement is to separate development and test functions from production functions. For example, a developer may use an administrator-level account with elevated privileges in the development environment, and have a separate account with user-level access to the production environment.	YES				
6.4.3 Production data (live PANs) are not used for testing or development	6.4.3.a Observe testing processes and interview personnel to verify procedures are in place to ensure production data (live PANs) are not used for testing or development. 6.4.3.b Examine a sample of test data to verify production data (live PANs) is not used for testing or development.	Security controls are usually not as stringent in test or development environments. Use of production data provides malicious individuals with the opportunity to gain unauthorized access to production data (cardholder data).	YES				

6.4.4 Removal of test data and accounts from system components before the system becomes active / goes into production.	6.4.4.a Observe testing processes and interview personnel to verify test data and accounts are removed before a production system becomes active. 6.4.4.b Examine a sample of data and accounts from production systems recently installed or updated to verify test data and accounts are removed before the system becomes active.	Test data and accounts should be removed from production code before the application becomes active, since these items may give away information about the functioning of the application or system. Possession of such information could facilitate compromise of the system and related cardholder data.	YES				
6.4.5 Change control procedures for the implementation of security patches and software modifications must include the following:	6.4.5.a Examine documented change control procedures related to implementing security patches and software modifications and verify procedures are defined for: - Documentation of impact - Documented change approval by authorized parties - Functionality testing to verify that the change does not adversely impact the security of the system - Back-out procedures 6.4.5.b For a sample of system components, interview responsible personnel to determine recent changes/security patches. Trace those changes back to related change control documentation. For each change examined, perform the following:	If not properly managed, the impact of software updates and security patches might not be fully realized and could have unintended consequences.	YES				
6.4.5.1 Documentation of impact.	6.4.5.1 Verify that documentation of impact is included in the change control documentation for each sampled change.	The impact of the change should be documented so that all affected parties can plan appropriately for any processing changes.	YES				
6.4.5.2 Documented change approval by authorized parties.	6.4.5.2 Verify that documented approval by authorized parties is present for each sampled change.	Approval by authorized parties indicates that the change is a legitimate and approved change sanctioned by the organization.	YES				
6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.	6.4.5.3.a For each sampled change, verify that functionality testing is performed to verify that the change does not adversely impact the security of the system. 6.4.5.3.b For custom code changes, verify that all updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production.	Thorough testing should be performed to verify that the security of the environment is not reduced by implementing a change. Testing should validate that all existing security controls remain in place, are replaced with equally strong controls, or are strengthened after any change to the environment.	YES				
6.4.5.4 Back-out procedures.	6.4.5.4 Verify that back-out procedures are prepared for each sampled change.	For each change, there should be documented back-out procedures in case the change fails or adversely affects the security of an application or system, to allow the system to be restored back to its previous state.	YES				
6.4.6 Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable. *Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*	6.4.6 For a sample of significant changes, examine change records, interview personnel, and observe the affected systems/networks to verify that applicable PCI DSS requirements were implemented and documentation updated as part of the change.	Having processes to analyze significant changes helps ensure that all appropriate PCI DSS controls are applied to any systems or networks added or changed within the in-scope environment. Building this validation into change management processes helps ensure that device inventories and configuration standards are kept up to date and security controls are applied where needed. A change management process should include supporting evidence that PCI DSS requirements are implemented or preserved through the iterative process. Examples of PCI DSS requirements that could be impacted include, but are not limited to: - Network diagram is updated to reflect changes. - Systems are configured per configuration standards, with all default passwords changed and unnecessary services disabled. - Systems are protected with required controls—e.g., file-integrity monitoring (FIM), anti-virus, patches, audit logging. -Sensitive authentication data (SAD) is not stored and all cardholder data (CHD) storage is documented and incorporated into data-retention policy and procedures - New systems are included in the quarterly vulnerability scanning process.	YES				
6.5 Address common coding vulnerabilities in software-development processes as follows: - Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities. - Develop applications based on secure coding guidelines. *Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS*	6.5.a Examine software-development policies and procedures to verify that training in secure coding techniques is required for developers, based on industry best practices and guidance. 6.5.b Examine records of training to verify that software developers receive up-to-date training on secure coding techniques at least annually, including how to avoid common coding vulnerabilities.	The application layer is high-risk and may be targeted by both internal and external threats. Requirements 6.5.1 through 6.5.10 are the minimum controls that should be in place, and organizations should incorporate the relevant secure coding practices as applicable to the particular technology in their environment. Application developers should be properly trained to identify and resolve issues related to these (and other) common coding vulnerabilities. Having staff knowledgeable of secure coding guidelines should minimize the number of security					

was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.	6.5.c Verify that processes are in place to protect applications from, at a minimum, the following vulnerabilities:	vulnerabilities introduced through poor coding practices. Training for developers may be provided in-house or by third parties and should be applicable for technology used. As industry-accepted secure coding practices change, organizational coding practices and developer training should likewise be updated to address new threats—for example, memory scraping attacks. The vulnerabilities identified in 6.5.1 through 6.5.10 provide a minimum baseline. It is up to the organization to remain up to date with vulnerability trends and incorporate appropriate measures into their secure coding practices.	YES				
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath injection flaws as well as other injection flaws.	6.5.1 Examine software-development policies and procedures and interview responsible personnel to verify that injection flaws are addressed by coding techniques that include: - Validating input to verify user data cannot modify meaning of commands and queries. - Utilizing parameterized queries.	Injection flaws, particularly SQL injection, are a commonly used method for compromising applications. Injection occurs when user-supplied data is sent to an interpreter as part of a command or query. The attacker's hostile data tricks the interpreter into executing unintended commands or changing data, and allows the attacker to attack components inside the network through the application, to initiate attacks such as buffer overflows, or to reveal both confidential information and server application functionality. Information should be validated before being sent to the application—for example, by checking for all alpha characters, mix of alpha and numeric characters, etc.	YES				
6.5.2 Buffer overflows	6.5.2 Examine software-development policies and procedures and interview responsible personnel to verify that buffer overflows are addressed by coding techniques that include: - Validating buffer boundaries. - Truncating input strings.	Buffer overflows occur when an application does not have appropriate bounds checking on its buffer space. This can cause the information in the buffer to be pushed out of the buffer's memory space and into executable memory space. When this occurs, the attacker has the ability to insert malicious code at the end of the buffer and then push that malicious code into executable memory space by overflowing the buffer. The malicious code is then executed and often enables the attacker remote access to the application and/or infected system.	YES				
6.5.3 Insecure cryptographic storage	6.5.3 Examine software-development policies and procedures and interview responsible personnel to verify that insecure cryptographic storage is addressed by coding techniques that: - Prevent cryptographic flaws. - Use strong cryptographic algorithms and keys.	Applications that do not utilize strong cryptographic functions properly to store data are at increased risk of being compromised, and exposing authentication credentials and/or cardholder data. If an attacker is able to exploit weak cryptographic processes, they may be able to gain clear-text access to encrypted data.	YES				
6.5.4 Insecure communications	6.5.4 Examine software-development policies and procedures and interview responsible personnel to verify that insecure communications are addressed by coding techniques that properly authenticate and encrypt all sensitive communications.	Applications that fail to adequately encrypt network traffic using strong cryptography are at increased risk of being compromised and exposing cardholder data. If an attacker is able to exploit weak cryptographic processes, they may be able to gain control of an application or even gain clear-text access to encrypted data.	YES				
6.5.5 Improper error handling	6.5.5 Examine software-development policies and procedures and interview responsible personnel to verify that improper error handling is addressed by coding techniques that do not leak information via error messages (for example, by returning generic rather than specific error details.	Applications can unintentionally leak information about their configuration or internal workings, or expose privileged information through improper error handling methods. Attackers use this weakness to steal sensitive data or compromise the system altogether. If a malicious individual can create errors that the application does not handle properly, they can gain detailed system information, create denial-of-service interruptions, cause security to fail, or crash the server. For example, the message "incorrect password provided" tells an attacker the user ID provided was accurate and that they should focus their efforts only on the password. Use more generic error messages, like "data could not be verified."	YES				
6.5.6 All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).	6.5.6 Examine software-development policies and procedures and interview responsible personnel to verify that coding techniques address any "high risk" vulnerabilities that could affect the application, as identified in PCI DSS Requirement 6.1.	All vulnerabilities identified by an organization's vulnerability risk-ranking process (defined in Requirement 6.1) to be "high risk" and that could affect the application should be identified and addressed during application development.	YES				
Note: Requirements 6.5.7 through 6.5.10, below, apply to web applications and application interfaces (internal or external):		Web applications, both internally and externally (public) facing, have unique security risks based upon their architecture as well as the relative ease and occurrence of compromise.	YES				

6.5.7 Cross-site scripting (XSS)	6.5.7 Examine software-development policies and procedures and interview responsible personnel to verify that cross-site scripting (XSS) is addressed by coding techniques that include - Validating all parameters before inclusion - Utilizing context-sensitive escaping.	XSS flaws occur whenever an application takes user-supplied data and sends it to a web browser without first validating or encoding that content. XSS allows attackers to execute script in the victim's browser, which can hijack user sessions, deface web sites, possibly introduce worms, etc.	YES				
6.5.8 Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).	6.5.8 Examine software-development policies and procedures and interview responsible personnel to verify that improper access control—such as insecure direct object references, failure to restrict URL access, and directory traversal—is addressed by coding technique that includes: - Proper authentication of users - Sanitizing input - Not exposing internal object references to users - User interfaces that do not permit access to unauthorized functions.	A direct object reference occurs when a developer exposes a reference to an internal implementation object, such as a file, directory, database record, or key, as a URL or form parameter. Attackers can manipulate those references to access other objects without authorization. Consistently enforce access control in presentation layer and business logic for all URLs. Frequently, the only way an application protects sensitive functionality is by preventing the display of links or URLs to unauthorized users. Attackers can use this weakness to access and perform unauthorized operations by accessing those URLs directly. An attacker may be able to enumerate and navigate the directory structure of a website (directory traversal) thus gaining access to unauthorized information as well as gaining further insight into the workings of the site for later exploitation. If user interfaces permit access to unauthorized functions, this access could result in unauthorized individuals gaining access to privileged credentials or cardholder data. Only authorized users should be permitted to access direct object references to sensitive resources. Limiting access to data resources will help prevent cardholder data from being presented to unauthorized resources.	YES				
6.5.9 Cross-site request forgery (CSRF)	6.5.9 Examine software development policies and procedures and interview responsible personnel to verify that cross-site request forgery (CSRF) is addressed by coding techniques that ensure applications do not rely on authorization credentials and tokens automatically submitted by browsers.	A CSRF attack forces a logged-on victim's browser to send a pre-authenticated request to a vulnerable web application, which then enables the attacker to perform any state-changing operations the victim is authorized to perform (such as updating account details, making purchases, or even authenticating to the application).	YES				
6.5.10 Broken authentication and session management *Note: Requirement 6.5.10 is a best practice until June 30, 2015, after which it becomes a requirement.*	6.5.10 Examine software development policies and procedures and interview responsible personnel to verify that broken authentication and session management are addressed via coding techniques that commonly include: - Flagging session tokens (for example cookies) as "secure" - Not exposing session IDs in the URL - Incorporating appropriate time-outs and rotation of session IDs after a successful login.	Secure authentication and session management prevents unauthorized individuals from compromising legitimate account credentials, keys, or session tokens that would otherwise enable the intruder to assume the identity of an authorized user.	YES				

6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: - Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes Note: This assessment is not the same as the vulnerability scans performed for Requirement 11.2. -Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.	6.6 For public-facing web applications, ensure that either one of the following methods is in place as follows: * Examine documented processes, interview personnel, and examine records of application security assessments to verify that public-facing web applications are reviewed—using either manual or automated vulnerability security assessment tools or methods—as follows: - At least annually - After any changes - By an organization that specializes in application security - That, at a minimum, all vulnerabilities in Requirement 6.5 are included in the assessment - That all vulnerabilities are corrected - That the application is re-evaluated after the corrections. * Examine the system configuration settings and interview responsible personnel to verify that an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) is in place as follows: - Is situated in front of public-facing web applications to detect and prevent web-based attacks. - Is actively running and up to date as applicable. - Is generating audit logs. - Is configured to either block web-based attacks, or generate an alert that is immediately investigated.	Public-facing web applications are primary targets for attackers, and poorly coded web applications provide an easy path for attackers to gain access to sensitive data and systems. The requirement for reviewing applications or installing web-application firewalls is intended to reduce the number of compromises on public-facing web applications due to poor coding or application management practices. * Manual or automated vulnerability security assessment tools or methods review and/or test the application for vulnerabilities * Web-application firewalls filter and block non-essential traffic at the application layer. Used in conjunction with a network-based firewall, a properly configured web-application firewall prevents application-layer attacks if applications are improperly coded or configured. This can be achieved through a combination of technology and process. Process-based solutions must have mechanisms that facilitate timely responses to alerts in order to meet the intent of this requirement, which is to prevent attacks. Note: "An organization that specializes in application security" can be either a third-party company or an internal organization, as long as the reviewers specialize in application security and can demonstrate independence from the development team.	YES				
6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.	6.7 Examine documentation and interview personnel to verify that security policies and operational procedures for developing and maintaining secure systems and applications are: - Documented, - In use, and - Known to all affected parties.	Personnel need to be aware of and following security policies and operational procedures to ensure systems and applications are securely developed and protected from vulnerabilities on a continuous basis.	YES				

Requirement 7: Restrict access to cardholder data by business need to know

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.
"Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.

PCI DSS Control Details			Control Responsibility				
PCI DSS Requirement	**Testing Procedure**	**Guidance**	**100% Service Provider**	**100% City of Vancouver**	**Shared**	**N/A**	**Please provide additional details where the City of Vancouver's PCI Environment may be impacted.**
Requirement 7: Restrict access to cardholder data by business need to know							
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	7.1 Examine written policy for access control, and verify that the policy incorporates 7.1.1 through 7.1.4 as follows: - Defining access needs and privilege assignments for each role - Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities - Assignment of access based on individual personnel's job classification and function - Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved.	The more people who have access to cardholder data, the more risk there is that a user's account will be used maliciously. Limiting access to those with a legitimate business reason for the access helps an organization prevent mishandling of cardholder data through inexperience or malice.				YES	We do not store any full or usable cardholder data, including expiration dates, CVV codes, PINS, and PANs.
7.1.1 Define access needs for each role, including: - System components and data resources that each role needs to access for their job function - Level of privilege required (for example, user, administrator, etc.) for accessing resources.	7.1.1 Select a sample of roles and verify access needs for each role are defined and include: - System components and data resources that each role needs to access for their job function - Identification of privilege necessary for each role to perform their job function.	In order to limit access to cardholder data to only those individuals who need such access, first it is necessary to define access needs for each role (for example, system administrator, call center personnel, store clerk), the systems/devices/data each role needs access to, and the level of privilege each role needs to effectively perform assigned tasks. Once roles and corresponding access needs are defined, individuals can be granted access accordingly.				YES	We do not store any full or usable cardholder data, including expiration dates, CVV codes, PINS, and PANs.
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	7.1.2.a Interview personnel responsible for assigning access to verify that access to privileged user IDs is: - Assigned only to roles that specifically require such privileged access - Restricted to least privileges necessary to perform job responsibilities. 7.1.2.b Select a sample of user IDs with privileged access and interview responsible management personnel to verify that privileges assigned are: - Necessary for that individual's job function - Restricted to least privileges necessary to perform job responsibilities.	When assigning privileged IDs, it is important to assign individuals only the privileges they need to perform their job (the "least privileges"). For example, the database administrator or backup administrator should not be assigned the same privileges as the overall systems administrator. Assigning least privileges helps prevent users without sufficient knowledge about the application from incorrectly or accidentally changing application configuration or altering its security settings. Enforcing least privilege also helps to minimize the scope of damage if an unauthorized person gains access to a user ID.				YES	We do not store any full or usable cardholder data, including expiration dates, CVV codes, PINS, and PANs.
7.1.3 Assign access based on individual personnel's job classification and function.	7.1.3 Select a sample of user IDs and interview responsible management personnel to verify that privileges assigned are based on that individual's job classification and function.	Once needs are defined for user roles (per PCI DSS requirement 7.1.1), it is easy to grant individuals access according to their job classification and function by using the already-created roles.	YES				
7.1.4 Require documented approval by authorized parties specifying required privileges.	7.1.4 Select a sample of user IDs and compare with documented approvals to verify that: - Documented approval exists for the assigned privileges - The approval was by authorized parties - That specified privileges match the roles assigned to the individual.	Documented approval (for example, in writing or electronically) assures that those with access and privileges are known and authorized by management, and that their access is necessary for their job function.	YES				

7.2 Establish an access control system for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:	7.2 Examine system settings and vendor documentation to verify that an access control system is implemented as follows:	Without a mechanism to restrict access based on user's need to know, a user may unknowingly be granted access to cardholder data. An access control system automates the process of restricting access and assigning privileges. Additionally, a default "deny-all" setting ensures no one is granted access until and unless a rule is established specifically granting such access. *Note: Some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.*	YES				
7.2.1 Coverage of all system components	7.2.1 Confirm that access control systems are in place on all system components.	Without a mechanism to restrict access based on user's need to know, a user may unknowingly be granted access to cardholder data. An access control system automates the process of restricting access and assigning privileges. Additionally, a default "deny-all" setting ensures no one is granted access until and unless a rule is established specifically granting such access. Note: Some access control systems are set by default to "allow-all," thereby	YES				
7.2.2 Assignment of privileges to individuals based on job classification and function.	7.2.2 Confirm that access control systems are configured to enforce privileges assigned to individuals based on job classification and function.						
7.2.3 Default "deny-all" setting.	7.2.3 Confirm that the access control systems have a default "deny-all" setting.						
7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.	7.3 Examine documentation interview personnel to verify that security policies and operational procedures for restricting access to cardholder data are: - Documented, - In use, and - Known to all affected parties.	Personnel need to be aware of and following security policies and operational procedures to ensure that access is controlled and based on need-to-know and least privilege, on a continuous basis.	YES				

Requirement 8: Identify and authenticate access to system components

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for their actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users and processes.

The effectiveness of a password is largely determined by the design and implementation of the authentication system—particularly, how frequently password attempts can be made by an attacker, and the security methods to protect user passwords at the point of entry, during transmission, and while in storage. Note: These requirements are applicable for all accounts, including point-of-sale accounts, with administrative capabilities and all accounts used to view or access cardholder data or to access systems with cardholder data. This includes accounts used by vendors and other third parties (for example, for support or maintenance). However, Requirements 8.1.1, 8.2, 8.5, 8.2.3 through 8.2.5, and 8.1.6 through 8.1.8 are not intended to apply to user accounts within a point-of-sale payment application that only have access to one card number at a time in order to facilitate a single transaction (such as cashier accounts).

PCI DSS Control Details			Control Responsibility				Please provide additional details where the City of Vancouver's PCI Environment may be impacted.
PCI DSS Requirement	Testing Procedure	Guidance	100% Service Provider	100% City of Vancouver	Shared	N/A	
Requirement 8: Assign a unique ID to each person with computer access							
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:	8.1.a Review procedures and confirm they define processes for each of the items below at 8.1.1 through 8.1.8	By ensuring each user is uniquely identified—instead of using one ID for several employees—an organization can maintain individual responsibility for actions and an effective audit trail per employee. This will help speed issue resolution and containment when misuse or malicious intent occurs.			YES		Customers have select users that are responsible for defining and documenting a User ID approval process, defining least privileges, restricting access to cardholder data, using unique IDs, providing separation of duties, and revoking user access when no longer necessary. There is no PCI access for Customers.
	8.1.b Verify that procedures are implemented for user identification management, by performing the following:						
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	8.1.1 Interview administrative personnel to confirm that all users are assigned a unique ID for access to system components or cardholder data.						
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	8.1.2 For a sample of privileged user IDs and general user IDs, examine associated authorizations and observe system settings to verify each user ID and privileged user ID has been implemented with only the privileges specified on the documented approval.	To ensure that user accounts granted access to systems are all valid and recognized users, strong processes must manage all changes to user IDs and other authentication credentials, including adding new ones and modifying or deleting existing ones.			YES		
8.1.3 Immediately revoke access for any terminated users.	8.1.3.a Select a sample of users terminated in the past six months, and review current user access lists—for both local and remote access—to verify that their IDs have been deactivated or removed from the access lists.	If an employee has left the company and still has access to the network via their user account, unnecessary or malicious access to cardholder data could occur—either by the former employee or by a malicious user who exploits the old and/or unused account. To prevent unauthorized access, user credentials and other authentication methods therefore need to be revoked promptly (as soon as possible) upon the employee's departure.			YES		
	8.1.3.b Verify all physical authentication methods—such as, smart cards, tokens, etc.—have been returned or deactivated.						
8.1.4 Remove/disable inactive user accounts within 90 days.	8.1.4 Observe user accounts to verify that any inactive accounts over 90 days old are either removed or disabled.	Accounts that are not used regularly are often targets of attack since it is less likely that any changes (such as a changed password) will be noticed. As such, these accounts may be more easily exploited and used to access cardholder data.	YES				
8.1.5 Manage IDs used by thid parties to access, support, or maintain system components via remote access as follows: - Enabled only during the time period needed and disabled when not in use. - Monitored when in use.	8.1.5.a Interview personnel and observe processes for managing accounts used by vendors to access, support, or maintain system components to verify that accounts used by vendors for remote access are: - Disabled when not in use - Enabled only when needed by the vendor, and disabled when not in use.	Allowing vendors to have 24/7 access into your network in case they need to support your systems increases the chances of unauthorized access, either from a user in the vendor's environment or from a malicious individual who finds and uses this always-available external entry point into your network. Enabling access only for the time periods needed, and disabling it as soon as it is no longer needed, helps prevent misuse of these connections. Monitoring of vendor access provides assurance that vendors are accessing only the systems necessary and only during approved time frames.			YES		IDs for 3rd parties are shared between Greenlots and Techmindz (Development) and SureCall (Call Center). They are reviewed and enabled only when in use. IDs are monitored, by Greenlots SOC, when in use.
	8.1.5.b Interview personnel and observe processes to verify that vendor remote access accounts are monitored while being used.						

8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.	8.1.6.a For a sample of system components, inspect system configuration settings to verify that authentication parameters are set to require that user accounts be locked out after not more than six invalid logon attempts. 8.1.6.b Additional testing procedure for service provider assessments only: Review internal processes and customer/user documentation, and observe implemented processes to verify that non-consumer customer user accounts are temporarily locked-out after not more than six invalid access attempts.	Without account-lockout mechanisms in place, an attacker can continually attempt to guess a password through manual or automated tools (for example, password cracking), until they achieve success and gain access to a user's account. Note: Testing Procedure 8.1.6.b is an additional procedure that only applies if the entity being assessed is a service provider.	YES				IDs for 3rd parties are shared between Greenlots and Techmindz (Development) and SureCall (Call Center). They are reviewed and enabled only when in use. IDs are monitored, by Greenlots SOC, when in use.		
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	8.1.7 For a sample of system components, inspect system configuration settings to verify that password parameters are set to require that once a user account is locked out, it remains locked for a minimum of 30 minutes or until a system administrator resets the account.	If an account is locked out due to someone continually trying to guess a password, controls to delay reactivation of these locked accounts stops the malicious individual from continually guessing the password (they will have to stop for a minimum of 30 minutes until the account is reactivated). Additionally, if reactivation must be requested, the admin or help desk can validate that it is the actual account owner requesting reactivation.	YES						
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	8.1.8 For a sample of system components, inspect system configuration settings to verify that system/session idle time out features have been set to 15 minutes or less.	When users walk away from an open machine with access to critical system components or cardholder data, that machine may be used by others in the user's absence, resulting in unauthorized account access and/or misuse. The re-authentication can be applied either at the system level to protect all sessions running on that machine, or at the application level.	YES						
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: - Something you know, such as a password or passphrase - Something you have, such as a token device or smart card - Something you are, such as a biometric.	8.2 To verify that users are authenticated using unique ID and additional authentication (for example, a password/phrase) for access to the cardholder data environment, perform the following: - Examine documentation describing the authentication method(s) used. - For each type of authentication method used and for each type of system component, observe an authentication to verify authentication is functioning consistent with documented authentication method(s).	These authentication methods, when used in addition to unique IDs, help protect users' IDs from being compromised, since the one attempting the compromise needs to know both the unique ID and the password (or other authentication used). Note that a digital certificate is a valid option for "something you have" as long as it is unique for a particular user. Since one of the first steps a malicious individual will take to compromise a system is to exploit weak or nonexistent passwords, it is important to implement good processes for authentication management.	YES						
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	8.2.1.a Examine vendor documentation and system configuration settings to verify that passwords are protected with strong cryptography during transmission 8.2.1.b For a sample of system components, examine password files to verify that passwords are unreadable during storage. 8.2.1.c For a sample of system components, examine data transmissions to verify that passwords are unreadable during transmission. 8.2.1.d Additional testing procedure for service provider assessments only: Observe password files to verify that non-consumer customer passwords are unreadable during storage. 8.2.1.e Additional testing procedure for service provider assessments only: Observe data transmissions to verify that non-consumer customer passwords are unreadable during transmission.	Many network devices and applications transmit unencrypted, readable passwords across the network and/or store passwords without encryption. A malicious individual can easily intercept unencrypted passwords during transmission using a "sniffer," or directly access unencrypted passwords in files where they are stored, and use this data to gain unauthorized access. Note: Testing Procedures 8.2.1.d and 8.2.1.e are additional procedures that only apply if the entity being assessed is a service provider.	YES						

8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.	8.2.2 Examine authentication procedures for modifying authentication credentials and observe security personnel to verify that, if a user requests a reset of an authentication credential by phone, e-mail, web, or other non-face-to-face method, the user's identity is verified before the authentication credential is modified.	Many malicious individuals use "social engineering"—for example, calling a help desk and acting as a legitimate user—to have a password changed so they can utilize a user ID. Consider use of a "secret question" that only the proper user can answer to help administrators identify the user prior to re-setting or modifying authentication credentials.	YES						
8.2.3 Passwords/phrases must meet the following: - Require a minimum length of at least seven characters. - Contain both numeric and alphabetic characters. Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.	8.2.3.a For a sample of system components, inspect system configuration settings to verify that user password parameters are set to require at least the following strength/complexity: - Require a minimum length of at least seven characters. - Contain both numeric and alphabetic characters. 8.2.3.b Additional testing procedure for service provider assessments only: Review internal processes and customer/user documentation to verify that non-consumer customer passwords are required to meet at least the following strength/complexity: - Require a minimum length of at least seven characters. - Contain both numeric and alphabetic characters.	Strong passwords/passphrases are the first line of defense into a network since a malicious individual will often first try to find accounts with weak or non-existent passwords. If passwords are short or simple to guess, it is relatively easy for a malicious individual to find these weak accounts and compromise a network under the guise of a valid user ID. This requirement specifies that a minimum of seven characters and both numeric and alphabetic characters should be used for passwords/passphrases. For cases where this minimum cannot be met due to technical limitations, entities can use "equivalent strength" to evaluate their alternative. For information on variability and equivalency of password strength (also referred to as entropy) for passwords/passphrases of different formats, refer to industry standards (e.g., the current version of NIST SP 800-63.) Note: Testing Procedure 8.2.3.b is an additional procedure that only applies if the entity being assessed is a service provider.	YES						
8.2.4 Change user passwords/passphrases at least once every 90 days.	8.2.4.a For a sample of system components, inspect system configuration settings to verify that user password parameters are set to require users to change passwords at least once every 90 days. 8.2.4.b Additional testing procedure for service provider assessments only: Review internal processes and customer/user documentation to verify that: □ Non-consumer customer user passwords are required to change periodically; and □ Non-consumer customer users are given guidance as to when, and under what circumstances, passwords must change.	Passwords/phrases that are valid for a long time without a change provide malicious individuals with more time to work on breaking the password/phrase. Note: Testing Procedure 8.2.4.b is an additional procedure that only applies if the entity being assessed is a service provider.	YES						
8.2.5 Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.	8.2.5.a For a sample of system components, obtain and inspect system configuration settings to verify that password parameters are set to require that new passwords cannot be the same as the four previously used 8.2.5.b Additional testing procedure for service provider assessments only: Review internal processes and customer/user documentation to verify that new non-consumer customer user passwords cannot be the same as the previous four passwords.	If password history isn't maintained, the effectiveness of changing passwords is reduced, as previous passwords can be reused over and over. Requiring that passwords cannot be reused for a period of time reduces the likelihood that passwords that have been guessed or brute-forced will be used in the future. Note: Testing Procedure 8.2.5.b is an additional procedure that only applies if the entity being assessed is a service provider.	YES						
8.2.6 Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.	8.2.6 Examine password procedures and observe security personnel to verify that first-time passwords for new users, and reset passwords for existing users, are set to a unique value for each user and changed after first use.	If the same password is used for every new user, an internal user, former employee, or malicious individual may know or easily discover this password, and use it to gain access to accounts.	YES						
8.3 Secure all individual non-console		Multi-factor authentication requires an individual to present a minimum							

administrative access and all remote access to the CDE using multi-factor authentication. Note: Multi-factor authentication requires that a minimum of two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.		of two separate forms of authentication (as described in Requirement 8.2), before access is granted. Multi-factor authentication provides additional assurance that the individual attempting to gain access is who they claim to be. With multi-factor authentication, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk. Multi-factor authentication is not required at both the system-level and application-level for a particular system component. Multi-factor authentication can be performed either upon authentication to the particular network or to the system component. Examples of multi-factor technologies include but are not limited to remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; and other technologies that facilitate multi-factor authentication.	YES						
8.3.1 Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access. *Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*	8.3.1.a Examine network and/or system configurations, as applicable, to verify multi-factor authentication is required for all non-console administrative access into the CDE. 8.3.1.b Observe a sample of administrator personnel login to the CDE and verify that at least two of the three authentication methods are used.	This requirement is intended to apply to all personnel with administrative access to the CDE. This requirement applies only to personnel with administrative access and only for non-console access to the CDE; it does not apply to application or system accounts performing automated functions. If the entity does not use segmentation to separate the CDE from the rest of their network, an administrator could use multi-factor authentication either when logging onto the CDE network or when logging onto a system. If the CDE is segmented from the rest of the entity's network, an administrator would need to use multi-factor authentication when connecting to a CDE system from a non-CDE network. Multi-factor authentication can be implemented at network level or at system/application level; it does not have to be both. If the administrator uses MFA when logging into the CDE network, they do not also need to use MFA to log into a particular system or application within the CDE.	YES						
8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside the entity's network.	8.3.2.a Examine system configurations for remote access servers and systems to verify multi-factor authentication is required for: - All remote access by personnel, both user and administrator, and - All third-party/vendor remote access including access to applications and system components for support or maintenance purposes). 8.3.2.b Observe a sample of personnel (for example, users and administrators) connecting remotely to the network and verify that at least two of the three authentication methods are used.	This requirement is intended to apply to all personnel—including general users, administrators, and vendors (for support or maintenance) with remote access to the network—where that remote access could lead to access to the CDE. If remote access is to an entity's network that has appropriate segmentation, such that remote users cannot access or impact the cardholder data environment, multi-factor authentication for remote access to that network would not be required. However, multi-factor authentication is required for any remote access to networks with access to the cardholder data environment, and is recommended for all remote access to the entity's networks.	YES YES				MFA's are utilized for authentication from any legitimate user outside Greenlots HQ or VPN (internal network) and for all admin/priveleged access.		
8.4 Document and communicate authentication procedures and policies and procedures to all users including:	8.4.a Examine procedures and interview personnel to verify that authentication procedures and policies are distributed to all users.	Communicating password/authentication procedures to all users helps those users understand and abide by the policies. For example, guidance on selecting strong passwords may include							

- Guidance on selecting strong authentication credentials - Guidance for how users should protect their authentication credentials - Instructions not to reuse previously used passwords - Instructions to change passwords if there is any suspicion the password could be compromised.	8.4.b Review authentication procedures and policies that are distributed to users and verify they include: - Guidance on selecting strong authentication credentials - Guidance for how users should protect their authentication credentials. - Instructions for users not to reuse previously used passwords - Instructions to change passwords if there is any suspicion the password could be compromised. 8.4.c Interview a sample of users to verify that they are familiar with authentication procedures and policies. 8.4.c Interview a sample of users to verify that they are familiar with authentication procedures and policies.	suggestions to help personnel select hard-to-guess passwords that don't contain dictionary words, and that don't contain information about the user (such as the user ID, names of family members, date of birth, etc.). Guidance for protecting authentication credentials may include not writing down passwords or saving them in insecure files, and being alert for malicious individuals who may attempt to exploit their passwords (for example, by calling an employee and asking for their password so the caller can "troubleshoot a problem"). Instructing users to change passwords if there is a chance the password is no longer secure can prevent malicious users from using a legitimate password to gain unauthorized access.	YES				Greenlots application provides password policy/rules. Authentication methods and password management is provided insdie application.		
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: - Generic user IDs are disabled or removed. - Shared user IDs do not exist for system administration and other critical functions. - Shared and generic user IDs are not used to administer any system components.	8.5.a For a sample of system components, examine user ID lists to verify the following: - Generic user IDs are disabled or removed. - Shared user IDs for system administration activities and other critical functions do not exist. - Shared and generic user IDs are not used to administer any system components. 8.5.b Examine authentication policies/procedures to verify that use of group and shared IDs and/or passwords or other authentication methods are explicitly prohibited. 8.5.c Interview system administrators to verify that group and shared IDs and/or passwords or other authentication methods are not distributed, even if requested.	If multiple users share the same authentication credentials (for example, user account and password), it becomes impossible to trace system access and activities to an individual. This in turn prevents an entity from assigning accountability for, or having effective logging of, an individual's actions, since a given action could have been performed by anyone in the group that has knowledge of the authentication credentials.			YES		Customer could choose to have a group-id/shared-id for administration of users. Greenlots does not use shared ids or group ids.		
8.5.1 Additional requirement for service providers only: Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer. Note: This requirement is not intended to apply to shared hosting providers accessing their own hosting environment, where multiple customer environments are hosted.	8.5.1 Additional testing procedure for service provider assessments only: Examine authentication policies and procedures and interview personnel to verify that different authentication credentials are used for access to each customer.	Note: This requirement applies only when the entity being assessed is a service provider. To prevent the compromise of multiple customers through the use of a single set of credentials, vendors with remote access accounts to customer environments should use a different authentication credential for each customer. Technologies, such as two-factor mechanisms, that provide a unique credential for each connection (for example, via a single-use password) could also meet the intent of this requirement.	YES						
8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: - Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. - Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.	8.6.a Examine authentication policies and procedures to verify that procedures for using authentication mechanisms such as physical security tokens, smart cards, and certificates are defined and include: - Authentication mechanisms are assigned to an individual account and not shared among multiple accounts. - Physical and/or logical controls are defined to ensure only the intended account can use that mechanism to gain access. 8.6.b Interview security personnel to verify authentication mechanisms are assigned to an account and not shared among multiple accounts. 8.6.c Examine system configuration settings and/or physical controls, as applicable, to verify that controls are implemented to ensure only the intended account can use that mechanism to gain access.	If user authentication mechanisms such as tokens, smart cards, and certificates can be used by multiple accounts, it may be impossible to identify the individual using the authentication mechanism. Having physical and/or logical controls (for example, a PIN, biometric data, or a password) to uniquely identify the user of the account will prevent unauthorized users from gaining access through use of a shared authentication mechanism.			YES				

8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: - All user access to, user queries of, and user actions on databases are through programmatic methods. - Only database administrators have the ability to directly access or query databases. - Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).	8.7.a Review database and application configuration settings and verify that all users are authenticated prior to access. 8.7.b Examine database and application configuration settings to verify that all user access to, user queries of, and user actions on (for example, move, copy, delete), the database are through programmatic methods only (for example, through stored procedures). 8.7.c Examine database access control settings and database application configuration settings to verify that user direct access to or queries of databases are restricted to database administrators. 8.7.d Examine database access control settings, database application configuration settings, and the related application IDs to verify that application IDs can only be used by the applications (and not by individual users or other processes).	Without user authentication for access to databases and applications, the potential for unauthorized or malicious access increases, and such access cannot be logged since the user has not been authenticated and is therefore not known to the system. Also, database access should be granted through programmatic methods only (for example, through stored procedures), rather than via direct access to the database by end users (except for DBAs, who may need direct access to the database for their administrative duties).				YES	The card data is never stored in full on our servers, and only a reference key (a unique identifier string unrelated to the payment card itself) is stored on our servers which is used to reference the payment card data which is stored securely on our 3rd party payment processor. We never store the full payment card number on our servers. We never store the payment card expiration date on our servers. We never store the authorization code otherwise known as the 'CVV' code on the back of the card on our servers. We never store the PIN of the payment card on our servers. Only the last 4 digits of the PAN are stored for display purposes, these are provided to us by the payment processor.		
8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.	8.8 Examine documentation interview personnel to verify that security policies and operational procedures for identification and authentication are: - Documented, - In use, and - Known to all affected parties.	Personnel need to be aware of and following security policies and operational procedures for managing identification and authorization on a continuous basis.			YES				

Requirement 9: Restrict physical access to cardholder data

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, "onsite personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises. A "visitor" refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. "Media" refers to all paper and electronic media containing cardholder data.

PCI DSS Control Details			Control Responsibility				Please provide additional details where the City of Vancouver's PCI Environment may be impacted.		
PCI DSS Requirement	**Testing Procedure**	**Guidance**	**100% Service Provider**	**100% City of Vancouver**	**Shared**	**N/A**			
Requirement 9: Restrict physical access to cardholder data									
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	9.1 Verify the existence of physical security controls for each computer room, data center, and other physical areas with systems in the cardholder data environment. - Verify that access is controlled with badge readers or other devices including authorized badges and lock and key. - Observe a system administrator's attempt to log into consoles for randomly selected systems in the cardholder environment and verify that they are "locked" to prevent unauthorized use.	Without physical access controls, such as badge systems and door controls, unauthorized persons could potentially gain access to the facility to steal, disable, disrupt, or destroy critical systems and cardholder data. Locking console login screens prevents unauthorized persons from gaining access to sensitive information, altering system configurations, introducing vulnerabilities into the network, or destroying records.	Yes						
9.1.1 Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. *Note: "Sensitive areas" refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.*	9.1.1.a Verify that video cameras and/or access control mechanisms are in place to monitor the entry/exit points to sensitive areas. 9.1.1.b Verify that video cameras and/or access control mechanisms are protected from tampering or disabling. 9.1.1.c Verify that video cameras and/or access control mechanisms are monitored and that data from cameras or other mechanisms is stored for at least three months.	When investigating physical breaches, these controls can help identify the individuals that physically accessed the sensitive areas, as well as when they entered and exited. Criminals attempting to gain physical access to sensitive areas will often attempt to disable or bypass the monitoring controls. To protect these controls from tampering, video cameras could be positioned so they are out of reach and/or be monitored to detect tampering. Similarly, access control mechanisms could be monitored or have physical protections installed to prevent them being damaged or disabled by malicious individuals. Examples of sensitive areas include corporate database server rooms, back-office rooms at retail locations that store cardholder data, and storage areas for large quantities of cardholder data. Sensitive areas should be identified by each organization to ensure the appropriate physical monitoring controls are implemented.	Yes						
9.1.2 Implement physical and/or logical controls to restrict access to publicly accessible network jacks. *For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.*	9.1.2 Interview responsible personnel and observe locations of publicly accessible network jacks to verify that physical and/or logical controls are in place to restrict access to publicly accessible network jacks.	Restricting access to network jacks (or network ports) will prevent malicious individuals from plugging into readily available network jacks and gain access into internal network resources. Whether logical or physical controls, or a combination of both, are used, they should be sufficient to prevent an individual or device that is not explicitly authorized from being able to connect to the network.	Yes						
9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	9.1.3 Verify that physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines is appropriately restricted.	Without security over access to wireless components and devices, malicious users could use an organization's unattended wireless devices to access network resources, or even connect their own devices to the wireless network to gain unauthorized access. Additionally, securing networking and communications hardware prevents malicious users from intercepting network traffic or physically connecting their own devices to wired network resources.	Yes						
9.2 Develop procedures to easily distinguish between onsite personnel and visitors, to include: - Identifying onsite personnel and visitors (for example, assigning badges) - Changes to access requirements - Revoking or terminating onsite personnel and expired visitor identification (such as ID badges)	9.2.a Review documented processes to verify that procedures are defined for identifying and distinguishing between onsite personnel and visitors. - Verify procedures include the following: - Identifying onsite personnel and visitors (for example, assigning badges), - Changing access requirements, and - Revoking terminated onsite personnel and expired visitor identification (such as ID badges)	Identifying authorized visitors so they are easily distinguished from onsite personnel prevents unauthorized visitors from being granted access to areas containing cardholder data.	Yes						

[illegible]	9.2.b Examine identification methods (such as ID badges) and observe processes for identifying and distinguishing between onsite personnel and visitors to verify that: - Visitors are clearly identified, and - It is easy to distinguish between onsite personnel and visitors.		Yes						
	9.2.c Verify that access to the identification process (such as a badge system) is limited to authorized personnel.		Yes						
9.3 Control physical access for onsite personnel to the sensitive areas as follows: - Access must be authorized and based on individual job function. - Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.	9.3.a For a sample of onsite personnel with physical access to the CDE, interview responsible personnel and observe access control lists to verify that: - Access to the CDE is authorized. - Access is required for the individual's job function.	Controlling physical access to the CDE helps ensure that only authorized personnel with a legitimate business need are granted access. When personnel leave the organization, all physical access mechanisms should be returned or disabled promptly (as soon as possible) upon their departure, to ensure personnel cannot gain physical access to the CDE once their employment has ended.	Yes						
	9.3.b Observe personnel access the CDE to verify that all personnel are authorized before being granted access.		Yes						
	9.3.c Select a sample of recently terminated employees and review access control lists to verify the personnel do not have physical access to sensitive areas.		Yes						
9.4 Implement procedures to identify and authorize visitors. Procedures should include the following:	9.4 Verify that visitor authorization and access controls are in place as follows:		Yes						
9.4.1 Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.	9.4.1.a Observe procedures and interview personnel to verify that visitors must be authorized before they are granted access to, and escorted at all times within, areas	Visitor controls are important to reduce the ability of unauthorized and malicious persons to gain access to facilities (and potentially, to cardholder data). Visitor controls ensure visitors are identifiable as visitors so personnel can monitor their activities, and that their access is restricted to just the duration of their legitimate visit. Ensuring that visitor badges are returned upon expiry or completion of the visit prevents malicious persons from using a previously authorized pass to gain physical access into the building after the visit has ended. A visitor log documenting minimum information on the visitor is easy and inexpensive to maintain and will assist in identifying physical access to a building or room, and potential access to cardholder data.	Yes						
	9.4.1.b Observe the use of visitor badges or other identification to verify that a physical token badge does not permit unescorted access to physical areas where cardholder data is processed or maintained.		Yes						
9.4.2 Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.	9.4.2.a Observe people within the facility to verify the use of visitor badges or other identification, and that visitors are easily distinguishable from onsite personnel.		Yes						
	9.4.2.b Verify that visitor badges or other identification expire.		Yes						
9.4.3 Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.	9.4.3 Observe visitors leaving the facility to verify visitors are asked to surrender their badge or other identification upon departure or expiration.		Yes						
9.4.4 A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless	9.4.4.a Verify that a visitor log is in use to record physical access to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted.		Yes						
	9.4.4.b Verify that the log contains: - The visitor's name, - The firm represented, and - The onsite personnel authorizing physical access.		Yes						
	9.4.4.c Verify that the log is retained for at least three months.		Yes						
9.5 Physically secure all media.	9.5 Verify that procedures for protecting cardholder data include controls for physically securing all media (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes).	Controls for physically securing media are intended to prevent unauthorized persons from gaining access to cardholder data on any type of media. Cardholder data is susceptible to unauthorized viewing, copying, or scanning if it is unprotected while it is on removable or portable media, printed out, or left on someone's desk.	Yes						
9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	9.5.1 Verify that the storage location security is reviewed at least annually to confirm that backup media sorage is secure.	If stored in a non-secured facility, backups that contain cardholder data may easily be lost, stolen, or copied for malicious intent. Periodically reviewing the storage facility enables the organization to address identified security issues in a timely manner, minimizing the potential risk.	Yes						
9.6 Maintain strict control over the internal or external distribution of any kind of media, including the following:	9.6 Verify that a policy exists to control distribution of media, and that the policy covers all distributed media including that distributed to individuals.	Procedures and processes help protect cardholder data on media distributed to internal and/or external users. Without such procedures data can be lost or stolen and used for fraudulent purposes.	Yes						
9.6.1 Classify media so the sensitivity of the data can be determined.	9.6.1 Verify that all media is classified so the sensitivity of the data can be determined.	It is important that media be identified such that its classification status can be easily discernible. Media not identified as confidential may not be adequately protected or may be lost or stolen. *Note: This does not mean the media needs to have a "Confidential" label attached; the intent is that the organization has identified media that contains sensitive data so it can protect it.*	Yes						
9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.	9.6.2.a Interview personnel and examine records to verify that all media sent outside the facility is logged and sent via secured courier or other delivery method that can be	Media may be lost or stolen if sent via a non-trackable method such as regular postal mail. Use of secure couriers to deliver any media that contains cardholder data allows organizations to use their tracking systems to maintain inventory and location of shipments.	Yes						
	9.6.2.b Select a recent sample of several days of offsite tracking logs for all media, and verify tracking details are documented.		Yes						

9.6.3 Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).	9.6.3 Select a recent sample of several days of offsite tracking logs for all media. From examination of the logs and interviews with responsible personnel, verify proper management authorization is obtained whenever media is moved from a secured area (including when media is distributed to individuals).	Without a firm process for ensuring that all media movements are approved before the media is removed from secure areas, the media would not be tracked or appropriately protected, and its location would be unknown, leading to lost or stolen media.	Yes				
9.7 Maintain strict control over the storage and accessibility of media.	9.7 Obtain and examine the policy for controlling storage and maintenance of all media and verify that the policy requires periodic media inventories.	Without careful inventory methods and storage controls, stolen or missing media could go unnoticed for an indefinite amount of time.	Yes				
9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.	9.7.1 Review media inventory logs to verify that logs are maintained and media inventories are performed at least annually.	If media is not inventoried, stolen or lost media may not be noticed for a long time or at all.	Yes				
9.8 Destroy media when it is no longer needed for business or legal reasons as follows:	9.8 Examine the periodic media destruction policy and verify that it covers all media and defines requirements for the following: - Hard-copy materials must be crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed. - Storage containers used for materials that are to be destroyed must be secured. - Cardholder data on electronic media must be rendered unrecoverable (e.g., via a secure wipe program in accordance with industry-accepted standards for secure deletion, or by physically destroying the media).	If steps are not taken to destroy information contained on hard disks, portable drives, CD/DVDs, or paper prior to disposal, malicious individuals may be able to retrieve information from the disposed media, leading to a data compromise. For example, malicious individuals may use a technique known as "dumpster diving," where they search through trashcans and recycle bins looking for information they can use to launch an attack. Securing storage containers used for materials that are going to be destroyed prevents sensitive information from being captured while the materials are being collected. For example, "to-be-shredded" containers could have a lock preventing access to its contents or physic ally prevent access to the inside of the container. Examples of methods for securely destroying electronic media include secure wiping, degaussing, or physical destruction (such as grinding or shredding hard disks).	Yes				
9.8.1 Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.	9.8.1.a Interview personnel and examine procedures to verify that hard-copy materials are crosscut shredded, incinerated, or pulped such that there is reasonable assurance the hard-copy materials cannot be reconstructed.		Yes				
	9.8.1.b Examine storage containers used for materials that contain information to be destroyed to verify that the containers are secured.		Yes				
9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	9.8.2 Verify that cardholder data on electronic media is rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise physically destroying the media).		Yes				
9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution. *Note: These requirements apply to card-reading devices used in card-present transactions (that is, card swipe or dip) at the point of sale. This requirement is not intended to apply to manual key-entry components such as computer keyboards and POS keypads.*	9.9 Examine documented policies and procedures to verify they include: - Maintaining a list of devices - Periodically inspecting devices to look for tampering or substitution - Training personnel to be aware of suspicious behavior and to report tampering or substitution of devices.	Criminals attempt to steal cardholder data by stealing and/or manipulating card-reading devices and terminals. For example, they will try to steal devices so they can learn how to break into them, and they often try to replace legitimate devices with fraudulent devices that send them payment card information every time a card is entered. Criminals will also try to add "skimming" components to the outside of devices, which are designed to capture payment card details before they even enter the device—for example, by attaching an additional card reader on top of the legitimate card reader so that the payment card details are captured twice: once by the criminal's component and then by the device's legitimate component. In this way, transactions may still be completed without interruption while the criminal is "skimming" the payment card information during the process. This requirement is recommended, but not required, for manual key-entry components such as computer keyboards and POS keypads. Additional best practices on skimming prevention are available on the PCI SSC website.	Yes				
9.9.1 Maintain an up-to-date list of devices. The list should include the following: - Make, model of device - Location of device (for example, the address of the site or facility where the device is located) - Device serial number or other method of unique identification.	9.9.1.a Examine the list of devices to verify it includes: - Make, model of device - Location of device (for example, the address of the site or facility where the device is located) - Device serial number or other method of unique identification.	Keeping an up-to-date list of devices helps an organization keep track of where devices are supposed to be, and quickly identify if a device is missing or lost. The method for maintaining a list of devices may be automated (for example, a device-management system) or manual (for example, documented in electronic or paper records). For on-the-road devices, the location may include the name of the personnel to whom the device is assigned.	Yes				
	9.9.1.b Select a sample of devices from the list and observe devices and device locations to verify that the list is accurate and up to date.		Yes				
	9.9.1.c Interview personnel to verify the list of devices is updated when devices are added, relocated, decommissioned, etc.		Yes				
9.9.2 Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device). *Note: Examples of signs that a device might have been tampered with or substituted include unexpected*	9.9.2.a Examine documented procedures to verify processes are defined to include the following: - Procedures for inspecting devices - Frequency of inspections.	Regular inspections of devices will help organizations to more quickly detect tampering or replacement of a device, and thereby minimize the potential impact of using fraudulent devices. The type of inspection will depend on the device—for example, photographs of devices that are known to be secure can be used to compare a device's current appearance with its original appearance to see whether it has changed. Another option may be to use a secure marker pen, such as a UV light marker, to mark device surfaces and device openings so any tampering or replacement will be apparent. Criminals will often replace	Yes				
	9.9.2.b Interview responsible personnel and observe inspection processes to verify: - Personnel are aware of procedures for inspecting devices. - All devices are periodically inspected for evidence of tampering and substitution.		Yes				

9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: - Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. - Do not install, replace, or return devices without verification. - Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). - Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	9.9.3.a Review training materials for personnel at point-of-sale locations to verify they include training in the following: - Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices - Not to install, replace, or return devices without verification - Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices) - Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	Criminals will often pose as authorized maintenance personnel in order to gain access to POS devices. All third parties requesting access to devices should always be verified before being provided access—for example, by checking with management or phoning the POS maintenance company (such as the vendor or acquirer) for verification. Many criminals will try to fool personnel by dressing for the part (for example, carrying toolboxes and dressed in work wear), and could also be knowledgeable about locations of devices, so it's important personnel are trained to follow procedures at all times. Another trick criminals like to use is to send a "new" POS system with instructions for swapping it with a legitimate system and "returning" the legitimate system to a specified address. The criminals may even provide return postage as they are very keen to get their hands on these devices. Personnel always verify with their manager or supplier that the device is legitimate and came from a trusted source before installing it or using it for business.	Yes				
	9.9.3.b Interview a sample of personnel at point-of-sale locations to verify they have received training and are aware of the procedures for the following: - Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices - Not to install, replace, or return devices without verification - Being aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices) - Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).		Yes				
9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.	9.10 Examine documentation and interview personnel to verify that security policies and operational procedures for restricting physical access to cardholder data are: - Documented, - In use, and - Known to all affected parties.	Personnel need to be aware of and following security policies and operational procedures for restricting physical access to cardholder data and CDE systems on a continuous basis.	Yes				

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

PCI DSS Control Details			Control Responsibility				
PCI DSS Requirement	**Testing Procedure**	**Guidance**	**100% Service Provider**	**100% City of Vancouver**	**Shared**	**N/A**	**Please provide additional details where the City of Vancouver's PCI Environment may be impacted.**
Requirement 10: Track and monitor all access to network resources and cardholder data							
10.1 Implement audit trails to link all access to system components to each individual user.	10.1 Verify, through observation and interviewing the system administrator, that: - Audit trails are enabled and active for system components. - Access to system components is linked to individual users.	It is critical to have a process or system that links user access to system components accessed. This system generates audit logs and provides the ability to trace back suspicious activity to a specific user.	YES				**Example:** Customers are responsible for recording and maintaining logs of all access by individual users to [Service provided by Third party Service Provider] by their personnel and systems.
10.2 Implement automated audit trails for all system components to reconstruct the following events:	10.2 Through interviews of responsible personnel, observation of audit logs, and examination of audit log settings, perform the following:	Generating audit trails of suspect activities alerts the system administrator, sends data to other monitoring mechanisms (like intrusion detection systems), and provides a history trail for post-incident follow-up. Logging of the following events enables an organization to identify and trace potentially malicious activities	YES				
10.2.1 All individual user accesses to cardholder data	10.2.1 Verify all individual access to cardholder data is logged.	Malicious individuals could obtain knowledge of a user account with access to systems in the CDE, or they could create a new, unauthorized account in order to access cardholder data. A record of all individual accesses to cardholder data can identify which accounts may have been compromised or misused.				YES	The card data is never stored in full on our servers, and only a reference key (a unique identifier string unrelated to the payment card itself) is stored on our servers which is used to reference the payment card data which is stored securely on our 3rd party payment processor. We never store the full payment card number on our servers. We never store the payment card expiration date on our servers. We never store the authorization code otherwise known as the 'CVV' code on the back of the card on our servers. We never store the PIN of the payment card on our servers. Only the last 4 digits of the PAN are stored for display purposes, these are provided to us by the payment processor.
10.2.2 All actions taken by any individual with root or administrative privileges	10.2.2 Verify all actions taken by any individual with root or administrative privileges are logged.	Accounts with increased privileges, such as the "administrator" or "root" account, have the potential to greatly impact the security or operational functionality of a system. Without a log of the activities performed, an organization is unable to trace any issues resulting from an administrative mistake or misuse of privilege back to the specific action and individual.	YES				
10.2.3 Access to all audit trails	10.2.3 Verify access to all audit trails is logged.	Malicious users often attempt to alter audit logs to hide their actions, and a record of access allows an organization to trace any inconsistencies or potential tampering of the logs to an individual account. Having access to logs identifying changes, additions, and deletions can help retrace steps made by unauthorized personnel.	YES				
10.2.4 Invalid logical access attempts	10.2.4 Verify invalid logical access attempts are logged.	Malicious individuals will often perform multiple access attempts on targeted systems. Multiple invalid login attempts may be an indication of an unauthorized user's attempts to "brute force" or guess a password.	YES				
10.2 5 Use of and changes to identification and authentication mechanisms—including but not limited to	10.2.5.a Verify use of identification and authentication mechanisms is logged.	Without knowing who was logged on at the time of an incident, it is impossible to identify the accounts that may have been used. Additionally,					

creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges	10.2.5.b Verify all elevation of privileges is logged. 10.2.5.c Verify all changes, additions, or deletions to any account with root or administrative privileges are logged.	malicious users may attempt to manipulate the authentication controls with the intent of bypassing them or impersonating a valid account.	YES						
10.2.6 Initialization, stopping, or pausing of the audit logs	10.2.6 Verify the following are logged: - Initialization of audit logs - Stopping or pausing of audit logs.	Turning the audit logs off (or pausing them) prior to performing illicit activities is a common practice for malicious users wishing to avoid detection. Initialization of audit logs could indicate that the log function was disabled by a user to hide their actions.	YES						
10.2.7 Creation and deletion of system-level objects	10.2.7 Verify creation and deletion of system level objects are logged.	Malicious software, such as malware, often creates or replaces system level objects on the target system in order to control a particular function or operation on that system. By logging when system-level objects, such as database tables or stored procedures, are created or deleted, it will be easier to determine whether such modifications were authorized.	YES						
10.3 Record at least the following audit trail entries for all system components for each event:	10.3 Through interviews and observation of audit logs, for each auditable event (from 10.2), perform the following:								
10.3.1 User identification	10.3.1 Verify user identification is included in log entries.	By recording these details for the auditable events at 10.2, a potential compromise can be quickly identified, and with sufficient detail to know who, what, where, when, and how.	YES						
10.3.2 Type of event	10.3.2 Verify type of event is included in log entries.								
10.3.3 Date and time	10.3.3 Verify date and time stamp is included in log entries.								
10.3.4 Success or failure indication	10.3.4 Verify success or failure indication is included in log entries.								
10.3.5 Origination of event	10.3.5 Verify origination of event is included in log entries.								
10.3.6 Identity or name of affected data, system component, or resource.	10.3.6 Verify identity or name of affected data, system component, or resources is included in log entries.								
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time: *Note: One example of time synchronization technology is Network Time Protocol (NTP).*	10.4 Examine configuration standards and processes to verify that time-synchronization technology is implemented and kept current per PCI DSS Requirements 6.1 and 6.2.								
10.4.1 Critical systems have the correct and consistent time.	10.4.1.a Examine the process for acquiring, distributing and storing the correct time within the organization to verify that: - Only the designated central time server(s) receives time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. - Where there is more than one designated time server, the time servers peer with one another to keep accurate time, - Systems receive time information only from designated central time server(s).	Time synchronization technology is used to synchronize clocks on multiple systems. When clocks are not properly synchronized, it can be difficult, if not impossible, to compare log files from different systems and establish an exact sequence of event (crucial for forensic analysis in the event of a breach). For post-incident forensics teams, the accuracy and consistency of time across all systems and the time of each activity is critical in determining how the systems were compromised.	YES						
	10.4.1.b Observe the time-related system-parameter settings for a sample of system components to verify: - Only the designated central time server(s) receives time signals from external sources, and time signals from external sources are based on International Atomic Time or UTC. - Where there is more than one designated time server, the designated central time server(s) peer with one another to keep accurate time. - Systems receive time only from designated central time server(s).								
10.4.2 Time data is protected.	10.4.2.a Examine system configurations and time-synchronization settings to verify that access to time data is restricted to only personnel with a business need to access time data.								
	10.4.2.b Examine system configurations, time synchronization settings and logs, and processes to verify that any changes to time settings on critical systems are logged, monitored, and reviewed.								

10.4.3 Time settings are received from industry-accepted time sources.	10.4.3 Examine systems configurations to verify that the time server(s) accept time updates from specific, industry-accepted external sources (to prevent a malicious individual from changing the clock). Optionally, those updates can be encrypted with a symmetric key, and access control lists can be created that specify the IP addresses of client machines that will be provided with the time updates (to prevent unauthorized use of internal time servers).								
10.5 Secure audit trails so they cannot be altered.	10.5 Interview system administrators and examine system configurations and permissions to verify that audit trails are secured so that they cannot be altered as follows:	Often a malicious individual who has entered the network will attempt to edit the audit logs in order to hide their activity. Without adequate protection of audit logs, their completeness, accuracy, and integrity cannot be guaranteed, and the audit logs can be rendered useless as an investigation tool after a compromise.	YES						
10.5.1 Limit viewing of audit trails to those with a job-related need.	10.5.1 Only individuals who have a job-related need can view audit trail files.	Adequate protection of the audit logs includes strong access control (limit access to logs based on "need to know" only), and use of physical or network segregation to make the logs harder to find and modify. Promptly backing up the logs to a centralized log server or media that is difficult to alter keeps the logs protected even if the system generating the logs becomes compromised.	YES						
10.5.2 Protect audit trail files from unauthorized modifications.	10.5.2 Current audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.								
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	10.5.3 Current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter.								
10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.	10.5.4 Logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) are written onto a secure, centralized, internal log server or media.	By writing logs from external-facing technologies such as wireless, firewalls, DNS, and mail servers, the risk of those logs being lost or altered is lowered, as they are more secure within the internal network. Logs may be written directly, or offloaded or copied from external systems, to the secure internal system or media.	YES						
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	10.5.5 Examine system settings, monitored files, and results from monitoring activities to verify the use of file-integrity monitoring or change-detection software on logs.	File-integrity monitoring or change-detection systems check for changes to critical files, and notify when such changes are noted. For file-integrity monitoring purposes, an entity usually monitors files that don't regularly change, but when changed indicate a possible compromise.	YES						
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. *Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.*	10.6 Perform the following:	Many breaches occur over days or months before being detected. Checking logs daily minimizes the amount of time and exposure of a potential breach. Regular log reviews by personnel or automated means can identify and proactively address unauthorized access to the cardholder data environment. The log review process does not have to be manual. The use of log harvesting, parsing, and alerting tools can help facilitate the process by identifying log events that need to be reviewed.	YES						
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. *Note: Log harvesting, parsing, and alerting tools may be used to meet this Requirement.*	10.6 Perform the following:	Many breaches occur over days or months before being detected. Regular log reviews by personnel or automated means can identify and proactively address unauthorized access to the cardholder data environment. The log review process does not have to be manual. The use of log harvesting, parsing, and alerting tools can help facilitate the process by identifying log events that need to be reviewed.	YES						
10.6.1 Review the following at least daily: - All security events - Logs of all system components that store, process, or transmit CHD and/or SAD - Logs of all critical system components - Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection	10.6.1.a Examine security policies and procedures to verify that procedures are defined for reviewing the following at least daily, either manually or via log tools: - All security events - Logs of all system components that store, process, or transmit CHD and/or SAD - Logs of all critical system components - Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.)	Checking logs daily minimizes the amount of time and exposure of a potential breach. Daily review of security events—for example, notifications or alerts that identify suspicious or anomalous activities—as well as logs from critical system components, and logs from systems that perform security functions, such as firewalls, IDS/IPS, file-integrity monitoring (FIM) systems, etc. is necessary to identify potential issues. Note that the determination of "security event" will vary for each organization and may include consideration for the type of technology, location, and function of	YES						

servers, etc.).	10.6.1.b Observe processes and interview personnel to verify that the following are reviewed at least daily: - All security events - Logs of all system components that store, process, or transmit CHD and/or SAD - Logs of all critical system components - Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	the device. Organizations may also wish to maintain a baseline of "normal" traffic to help identify anomalous behavior.	YES						
10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.	10.6.2.a Examine security policies and procedures to verify that procedures are defined for reviewing logs of all other system components periodically—either manually or via log tools—based on the organization's policies and risk management strategy. 10.6.2.b Examine the organization's risk-assessment documentation and interview personnel to verify that reviews are performed in accordance with organization's policies and risk management strategy.	Logs for all other system components should also be periodically reviewed to identify indications of potential issues or attempts to gain access to sensitive systems via less-sensitive systems. The frequency of the reviews should be determined by an entity's annual risk assessment.	YES						
10.6.3 Follow up exceptions and anomalies identified during the review process.	10.6.3.a Examine security policies and procedures to verify that procedures are defined for following up on exceptions and anomalies identified during the review process. 10.6.3.b Observe processes and interview personnel to verify that follow-up to exceptions and anomalies is performed.	If exceptions and anomalies identified during the log-review process are not investigated, the entity may be unaware of unauthorized and potentially malicious activities that are occurring within their own network.	YES						
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	10.7.a Examine security policies and procedures to verify that they define the following: - Audit log retention policies - Procedures for retaining audit logs for at least one year, with a minimum of three months immediately available online. 10.7.b Interview personnel and examine audit logs to verify that audit logs are available for at least one year. 10.7.c Interview personnel and observe processes to verify that at least the last three months' logs can be immediately restored for analysis.	Retaining logs for at least a year allows for the fact that it often takes a while to notice that a compromise has occurred or is occurring, and allows investigators sufficient log history to better determine the length of time of a potential breach and potential system(s) impacted. By having three months of logs immediately available, an entity can quickly identify and minimize impact of a data breach. Storing logs in off-line locations could prevent them from being readily available, resulting in longer time frames to restore log data, perform analysis, and identify impacted systems or data.	YES						
10.8 Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: - Firewalls - IDS/IPS - FIM - Anti-virus - Physical access controls - Logical access controls - Audit logging mechanisms - Segmentation controls (if used) Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.	10.8.a Examine documented policies and procedures to verify that processes are defined for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: -Firewalls - IDS/IPS - FIM - Anti-virus - Physical access controls - Logical access controls - Audit logging mechanisms - Segmentation controls (if used) 10.8.b Examine detection and alerting processes and interview personnel to verify that processes are implemented for all critical security controls, and that failure of a critical security control results in the generation of an alert.	Note: This requirement applies only when the entity being assessed is a service provider. Without formal processes to detect and alert when critical security controls fail, failures may go undetected for extended periods and provide attackers ample time to compromise systems and steal sensitive data from the cardholder data environment. The specific types of failures may vary depending on the function of the device and technology in use. Typical failures include a system ceasing to perform its security function or not functioning in its intended manner; for example, a firewall erasing all its rules or going offline.	YES						

10.8.1 Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: - Restoring security functions - Identifying and documenting the duration (date and time start to end) of the security failure - Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause - Identifying and addressing any security issues that arose during the failure - Performing a risk assessment to determine whether further actions are required as a result of the security failure - Implementing controls to prevent cause of failure from reoccurring -Resuming monitoring of security controls Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.	10.8.1.a Examine documented policies and procedures and interview personnel to verify processes are defined and implemented to respond to a security control failure, and include: - Restoring security functions - Identifying and documenting the duration (date and time start to end) of the security failure - Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause - Identifying and addressing any security issues that arose during the failure - Performing a risk assessment to determine whether further actions are required as a result of the security failure - Implementing controls to prevent cause of failure from reoccurring - Resuming monitoring of security controls	Note: This requirement applies only when the entity being assessed is a service provider. If critical security control failures alerts are not quickly and effectively responded to, attackers may use this time to insert malicious software, gain control of a system, or steal data from the entity's environment. Documented evidence (e.g., records within a problem management system) should support that processes and procedures are in place to respond to security failures. In addition, personnel should be aware of their responsibilities in the event of a failure. Actions and responses to the failure should be captured in the documented evidence.	YES						
	10.8.1.b Examine records to verify that security control failures are documented to include: - Identification of cause(s) of the failure, including root cause - Duration (date and time start and end) of the security failure - Details of the remediation required to address the root cause								
10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.	10.9 Examine documentation and interview personnel to verify that security policies and operational procedures for monitoring all access to network resources and cardholder data are: - Documented, - In use, and - Known to all affected parties.	Personnel need to be aware of and following security policies and daily operational procedures for monitoring all access to network resources and cardholder data on a continuous basis.	YES				The card data is never stored in full on our servers, and only a reference key (a unique identifier string unrelated to the payment card itself) is stored on our servers which is used to reference the payment card data which is stored securely on our 3rd party payment processor. We never store the full payment card number on our servers. We never store the payment card expiration date on our servers. We never store the authorization code otherwise known as the 'CVV' code on the back of the card on our servers. We never store the PIN of the payment card on our servers. Only the last 4 digits of the PAN are stored for display purposes, these are provided to us by the payment processor.		

Requirement 11: Regularly test security systems and processes.
Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.

PCI DSS Control Details			Control Responsibility				
PCI DSS Requirement	**Testing Procedure**	**Guidance**	**100% Service Provider**	**100% City of Vancouver**	**Shared**	**N/A**	**Please provide additional details where the City of Vancouver's PCI Environment may be impacted.**
Requirement 11: Regularly test security systems and processes							
11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis. *Note: Methods that may be used in the process include but are not limited to wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS.* *Whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices.*	11.1.a Examine policies and procedures to verify processes are defined for detection and identification of both authorized and unauthorized wireless access points on a quarterly basis.	Implementation and/or exploitation of wireless technology within a network are some of the most common paths for malicious users to gain access to the network and cardholder data. If a wireless device or network is installed without a company's knowledge, it can allow an attacker to easily and "invisibly" enter the network. Unauthorized wireless devices may be hidden within or attached to a computer or other system component, or be attached directly to a network port or network device, such as a switch or router. Any such unauthorized device could result in an unauthorized access point into the environment. Knowing which wireless devices are authorized can help administrators quickly identify non-authorized wireless devices, and responding to the identification of unauthorized wireless access points helps to proactively minimize the exposure of CDE to malicious individuals. Due to the ease with which a wireless access point can be attached to a network, the difficulty in detecting their presence, and the increased risk presented by unauthorized wireless devices, these processes must be performed even when a policy exists prohibiting the use of wireless technology. The size and complexity of a particular environment will dictate the appropriate tools and processes to be used to provide sufficient assurance that a rogue wireless access point has not been installed in the environment. For example: In the case of a single standalone retail kiosk in a shopping mall, where all communication components are contained within tamper-resistant and tamper-evident casings, performing a detailed physical inspection of the kiosk itself may be sufficient to provide assurance that a rogue wireless access point has not been attached or installed. However, in an environment with multiple nodes (such as in a large retail store, call center, server room or data center), detailed physical inspection is difficult. In this case, multiple methods may be combined to meet the requirement, such as performing physical system inspections in conjunction with the results of a wireless analyzer.	YES				
	11.1.b Verify that the methodology is adequate to detect and identify any unauthorized wireless access points, including at least the following: - WLAN cards inserted into system components - Portable or mobile devices attached to system components to create a wireless access point (for example, by USB, etc.) - Wireless devices attached to a network port or network device.						
	11.1.c If wireless scanning is utilized, examine output from recent wireless scans to verify that: - Authorized and unauthorized wireless access points are identified, and - The scan is performed at least quarterly for all system components and facilities.						
	11.1.d If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), verify the configuration will generate alerts to notify personnel.						
11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.	11.1.1 Examine documented records to verify that an inventory of authorized wireless access points is maintained and a business justification is documented for all authorized wireless access points.						
11.1.2 Implement incident response procedures in the event unauthorized wireless access points are detected.	11.1.2.a Examine the organization's incident response plan (Requirement 12.10) to verify it defines and requires a response in the event that an unauthorized wireless access point is detected.						
	11.1.2.b Interview responsible personnel and/or inspect recent wireless scans and related responses to verify action is taken when unauthorized wireless access points are found.						

11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). *Note: Multiple scan reports can be combined for the quarterly scan process to show that all systems were scanned and all applicable vulnerabilities have been addressed. Additional documentation may be required to verify non-remediated vulnerabilities are in the process of being addressed.* *For initial PCI DSS compliance, it is not required that four quarters of passing scans be completed if the assessor verifies 1) the most recent scan result was a passing scan, 2) the entity has documented policies and procedures requiring quarterly scanning, and 3) vulnerabilities noted in the scan results have been corrected as shown in a re-scan(s). For subsequent years after the initial PCI DSS review, four quarters of passing scans must have occurred.*	11.2 Examine scan reports and supporting documentation to verify that internal and external vulnerability scans are performed as follows:	A vulnerability scan is a combination of automated or manual tools, techniques, and/or methods run against external and internal network devices and servers, designed to expose potential vulnerabilities that could be found and exploited by malicious individuals. There are three types of vulnerability scanning required for PCI DSS: - Internal quarterly vulnerability scanning by qualified personnel (use of a PCI SSC Approved Scanning Vendor (ASV) is not required) - External quarterly vulnerability scanning, which must be performed by an ASV - Internal and external scanning as needed after significant changes Once these weaknesses are identified, the entity corrects them and repeats the scan until all vulnerabilities have been corrected. Identifying and addressing vulnerabilities in a timely manner reduces the likelihood of a vulnerability being exploited and potential compromise of a system component or cardholder data.	YES				
11.2.1 Perform quarterly internal vulnerability scans and rescans as needed, until all "high-risk" vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel.	11.2.1.a Review the scan reports and verify that four quarterly internal scans occurred in the most recent 12-month period. 11.2.1.b Review the scan reports and verify that the scan process includes rescans until all "high-risk" vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved. 11.2.1.c Interview personnel to verify that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	An established process for identifying vulnerabilities on internal systems requires that vulnerability scans be conducted quarterly. Vulnerabilities posing the greatest risk to the environment (for example, ranked "High" per Requirement 6.1) should be resolved with the highest priority. Internal vulnerability scans can be performed by qualified, internal staff that are reasonably independent of the system component(s) being scanned (for example, a firewall administrator should not be responsible for scanning the firewall), or an entity may choose to have internal vulnerability scans performed by a firm specializing in vulnerability scanning.	YES				
11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved. *Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). Refer to the ASV Program Guide published on the PCI SSC*	11.2.2.a Review output from the four most recent quarters of external vulnerability scans and verify that four quarterly external vulnerability scans occurred in the most recent 12-month period. 11.2.2.b Review the results of each quarterly scan and rescan to verify that the ASV Program Guide requirements for a passing scan have been met (for example, no vulnerabilities rated 4.0 or higher by the CVSS, and no automatic failures). 11.2.2.c Review the scan reports to verify that the scans were completed by a PCI SSC Approved Scanning Vendor (ASV).	As external networks are at greater risk of compromise, quarterly external vulnerability scanning must be performed by a PCI SSC Approved Scanning Vendor (ASV). A robust scanning program ensures that scans are performed and vulnerabilities addressed in a timely manner.	YES				
11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.	11.2.3.a Inspect and correlate change control documentation and scan reports to verify that system components subject to any significant change were scanned. 11.2.3.b Review scan reports and verify that the scan process includes rescans until: - For external scans, no vulnerabilities exist that are scored 4.0 or higher by the CVSS. - For internal scans, all "high-risk" vulnerabilities as defined in PCI DSS Requirement 6.1 are resolved. 11.2.3.c Validate that the scan was performed by a qualified internal resource(s) or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	The determination of what constitutes a significant change is highly dependent on the configuration of a given environment. If an upgrade or modification could allow access to cardholder data or affect the security of the cardholder data environment, then it could be considered significant. Scanning an environment after any significant changes are made ensures that changes were completed appropriately such that the security of the environment was not compromised as a result of the change. All system components affected by the change will need to be scanned.	YES				

11.3 Implement a methodology for penetration testing that includes the following: - Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) - Includes coverage for the entire CDE perimeter and critical systems - Includes testing from both inside and outside the network - Includes testing to validate any segmentation and scope-reduction controls - Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 - Defines network-layer penetration tests to include components that support network functions as well as operating systems - Includes review and consideration of threats and vulnerabilities experienced in the last 12 months - Specifies retention of penetration testing results and remediation activities results.	11.3 Examine penetration-testing methodology and interview responsible personnel to verify a methodology is implemented that includes the following: - Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) - Includes coverage for the entire CDE perimeter and critical systems - Testing from both inside and outside the network - Includes testing to validate any segmentation and scope-reduction controls - Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 - Defines network-layer penetration tests to include components that support network functions as well as operating systems - Includes review and consideration of threats and vulnerabilities experienced in the last 12 months - Specifies retention of penetration testing results and remediation activities results.	The intent of a penetration test is to simulate a real-world attack situation with a goal of identifying how far an attacker would be able to penetrate into an environment. This allows an entity to gain a better understanding of their potential exposure and develop a strategy to defend against attacks. A penetration test differs from a vulnerability scan, as a penetration test is an active process that may include exploiting identified vulnerabilities. Conducting a vulnerability scan may be one of the first steps a penetration tester will perform in order to plan the testing strategy, although it is not the only step. Even if a vulnerability scan does not detect known vulnerabilities, the penetration tester will often gain enough knowledge about the system to identify possible security gaps. Penetration testing is generally a highly manual process. While some automated tools may be used, the tester uses their knowledge of systems to penetrate into an environment. Often the tester will chain several types of exploits together with a goal of breaking through layers of defenses. For example, if the tester finds a means to gain access to an application server, they will then use the compromised server as a point to stage a new attack based on the resources the server has access to. In this way, a tester is able to simulate the methods performed by an attacker to identify areas of potential weakness in the environment. Penetration testing techniques will be different for different organizations, and the type, depth, and complexity of the testing will depend on the specific environment and the organization's risk assessment.	YES				Alert Logic and 3rd party penetrationt tests resulted in certain gaps which are corrected or in process of being corrected.
11.3.1 Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	11.3.1.a Examine the scope of work and results from the most recent external penetration test to verify that penetration testing is performed as follows: - Per the defined methodology - At least annually - After any significant changes to the environment.	Penetration testing conducted on a regular basis and after significant changes to the environment is a proactive security measure that helps minimize potential access to the CDE by malicious individuals. The determination of what constitutes a significant upgrade or modification is highly dependent on the configuration of a given environment. If an upgrade or modification could allow access to cardholder data or affect the security of the cardholder data environment, then it could be considered significant. Performing penetration tests after network upgrades and modifications provides assurance that the controls assumed to be in place are still working effectively after the upgrade or modification.	YES				
	11.3.1.b Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).						
11.3.2 Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	11.3.2.a Examine the scope of work and results from the most recent internal penetration test to verify that penetration testing is performed as follows. -Per the defined methodology - At least annually - After any significant changes to the environment.						
	11.3.2.b Verify that the test was performed by a qualified internal resource or qualified external third party, and if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).						
11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.	11.3.3 Examine penetration testing results to verify that noted exploitable vulnerabilities were corrected and that repeated testing confirmed the vulnerability was corrected.						
11.3.4 If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	11.3.4.a Examine segmentation controls and review penetration-testing methodology to verify that penetration-testing procedures are defined to test all segmentation methods to confirm they are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	Penetration testing is an important tool to confirm that any segmentation in place to isolate the CDE from other networks is effective. The penetration testing should focus on the segmentation controls, both from outside the entity's network and from inside the network but outside of the CDE, to confirm that they are not able to get through the segmentation controls to access the CDE. For example, network testing and/or scanning for open ports, to verify no connectivity between in-scope and out-of-scope networks.	YES				
	11.3.4.b Examine the results from the most recent penetration test to verify that: - Penetration testing to verify segmentation controls is performed at least annually and after any changes to segmentation controls/methods. - The penetration testing covers all segmentation controls/methods in use. - The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.						
	11.3.4.c Verify that the test was performed by a qualified internal resource or qualified external third party and, if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).						

11.3.4.1 Additional requirement for service providers only: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods. Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.	11.3.4.1.a Examine the results from the most recent penetration test to verify that: - Penetration testing is performed to verify segmentation controls at least every six months and after any changes to segmentation controls/methods. - The penetration testing covers all segmentation controls/methods in use. - The penetration testing verifies that segmentation controls/methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE. 11.3.4.1.b Verify that the test was performed by a qualified internal resource or qualified external third party and, if applicable, organizational independence of the tester exists (not required to be a QSA or ASV).	Note: This requirement applies only when the entity being assessed is a service provider. For service providers, validation of PCI DSS scope should be performed as frequently as possible to ensure PCI DSS scope remains up to date and aligned with changing business objectives.	YES				Greenlots uses a 3rd party to conduct penetration testing every year. Results can be shared if needed
11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.	11.4.a Examine system configurations and network diagrams to verify that techniques (such as intrusion-detection systems and/or intrusion-prevention systems) are in place to monitor all traffic: - At the perimeter of the cardholder data environment - At critical points in the cardholder data environment. 11.4.b Examine system configurations and interview responsible personnel to confirm intrusion-detection and/or intrusion-prevention techniques alert personnel of suspected compromises. 11.4.c Examine IDS/IPS configurations and vendor documentation to verify intrusion-detection and/or intrusion-prevention techniques are configured, maintained, and updated per vendor instructions to ensure optimal protection.	Intrusion detection and/or intrusion prevention techniques (such as IDS/IPS) compare the traffic coming into the network with known "signatures" and/or behaviors of thousands of compromise types (hacker tools, Trojans, and other malware), and send alerts and/or stop the attempt as it happens. Without a proactive approach to unauthorized activity detection, attacks on (or misuse of) computer resources could go unnoticed in real time. Security alerts generated by these techniques should be monitored so that the attempted intrusions can be stopped.	YES				AlertLogic sends alerts for malware and intrusion detection. Dev Ops team is alerted and appropriate measures are taken to block the attack.
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. *Note: For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured*	11.5.a Verify the use of a change-detection mechanism within the cardholder data environment by observing system settings and monitored files, as well as reviewing results from monitoring activities. Examples of files that should be monitored: - System executables - Application executables - Configuration and parameter files - Centrally stored, historical or archived, log and audit files - Additional critical files determined by entity (for example, through risk assessment or other means). 11.5.b Verify the mechanism is configured to alert personnel to unauthorized modification (including changes, additions, and deletions) of critical files, and to perform critical file comparisons at least weekly.	Change-detection solutions such as file-integrity monitoring (FIM) tools check for changes, additions, and deletions to critical files, and notify when such changes are detected. If not implemented properly and the output of the change-detection solution monitored, a malicious individual could add, remove, or alter configuration file contents, operating system programs, or application executables. Unauthorized changes, if undetected, could render existing security controls ineffective and/or result in cardholder data being stolen with no perceptible impact to normal processing.	YES				AlertLogic used to monitor system for unwarranted changes.
11.5.1 Implement a process to respond to any alerts generated by the change-detection solution.	11.5.1 Interview personnel to verify that all alerts are investigated and resolved.						
11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.	11.6 Examine documentation interview personnel to verify that security policies and operational procedures for security monitoring and testing are: - Documented, - In use, and - Known to all affected parties.	Personnel need to be aware of and following security policies and operational procedures for security monitoring and testing on a continuous basis.	YES				

Requirement 12: Maintain a policy that addresses information security for all personnel.
A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, "personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are "resident" on the entity's site or otherwise have access to the cardholder data environment.

PCI DSS Control Details			Control Responsibility				
PCI DSS Requirement	**Testing Procedure**	**Guidance**	**100% Service Provider**	**100% City of Vancouver**	**Shared**	**N/A**	**Please provide additional details where the City of Vancouver's PCI Environment may be impacted.**
Requirement 12: Maintain a policy that addresses information security for all personnel							
12.1 Establish, publish, maintain, and disseminate a security policy.	12.1 Examine the information security policy and verify that the policy is published and disseminated to all relevant personnel (including vendors and business partners).	A company's information security policy creates the roadmap for implementing security measures to protect its most valuable assets. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it.	YES				GreenLots works with a set of ISO Domain related security policies, created with ISO 27001 compliance.
12.1.1 Review the security policy at least annually and update the policy when the environment changes.	12.1.1 Verify that the information security policy is reviewed at least annually and updated as needed to reflect changes to business objectives or the risk environment.	Security threats and protection methods evolve rapidly. Without updating the security policy to reflect relevant changes, new protection measures to fight against these threats are not addressed.	YES				GreenLots reviews policies at least annually.
12.2 Implement a risk-assessment process that: - Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), - Identifies critical assets, threats, and vulnerabilities, and - Results in a formal, documented analysis of risk. Examples of risk-assessment methodologies include but	12.2.a Verify that an annual risk-assessment process is documented that: - Identifies critical assets, threats, and vulnerabilities 12.2.b Review risk-assessment documentation to verify that the risk-assessment process is performed at least annually and upon significant changes to the environment.	A risk assessment enables an organization to identify threats and associated vulnerabilities with the potential to negatively impact their business. Resources can then be effectively allocated to implement controls that reduce the likelihood and/or the potential impact of the threat being realized. Performing risk assessments at least annually and upon significant changes allows the organization to keep up to date with organizational changes and evolving threats, trends, and technologies.	YES				GreenLots, as mentioned, works with a set of ISO Domain policies, and also publishes critical procedures aligned with such.
12.3 Develop usage policies for critical technologies and define proper use of these technologies. *Note: Examples of critical technologies include, but are not limited to, remote access and wireless technologies, laptops, tablets, removable electronic media, e-mail usage and Internet usage.* Ensure these usage policies require the following:	12.3 Examine the usage policies for critical technologies and interview responsible personnel to verify the following policies are implemented and followed:	Personnel usage policies can either prohibit use of certain devices and other technologies if that is company policy, or provide guidance for personnel as to correct usage and implementation. If usage policies are not in place, personnel may use the technologies in violation of company policy, thereby allowing malicious individuals to gain access to critical systems and cardholder data.	YES				GreenLots, as mentioned, works with a set of ISO Domain policies, and also publishes critical procedures aligned with such.
12.3.1 Explicit approval by authorized parties	12.3.1 Verify that the usage policies include processes for explicit approval from authorized parties to use the technologies.	Without requiring proper approval for implementation of these technologies, individual personnel may innocently implement a solution to a perceived business need, but also open a huge hole that subjects critical systems and data to malicious individuals.	YES				GreenLots has a Change Management Policy and approval process.
12.3.2 Authentication for use of the technology	12.3.2 Verify that the usage policies include processes for all technology use to be authenticated with user ID and password or other authentication item (for example, token).	If technology is implemented without proper authentication (user IDs and passwords, tokens, VPNs, etc.), malicious individuals may easily use this unprotected technology to access critical systems and cardholder data.	YES				Greenlots has deployed VPN and MFA for priveleged users.
12.3.3 A list of all such devices and personnel with access	12.3.3 Verify that the usage policies define a list of all devices and personnel authorized to use the devices.	Malicious individuals may breach physical security and place their own devices on the network as a "back door." Personnel may also bypass procedures and install devices. An accurate inventory with proper device labeling allows for quick identification of non-approved installations.	YES				GreenLots has both Corp and Services asset inventory and labeling.

12.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)	12.3.4 Verify that the usage policies define a method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices).	Malicious individuals may breach physical security and place their own devices on the network as a "back door." Personnel may also bypass procedures and install devices. An accurate inventory with proper device labeling allows for quick identification of non-approved installations. Consider establishing an official naming convention for devices, and log all devices with established inventory controls. Logical labeling may be employed with information such as codes that can correlate the device to its owner, contact information, and purpose.	YES				GreenLots has both Corp and Services asset inventory and labeling.
12.3.5 Acceptable uses of the technology	12.3.5 Verify that the usage policies define acceptable uses for the technology.	By defining acceptable business use and location of company-approved devices and technology, the company is better able to manage and control gaps in configurations and operational controls, to ensure a "back door" is not opened for a malicious individual to gain access to critical systems and cardholder data.	YES				GreenLots has an acceptable use policy that defines devices, uses and locations.
12.3.6 Acceptable network locations for the technologies	12.3.6 Verify that the usage policies define acceptable network locations for the technology.						
12.3.7 List of company-approved products	12.3.7 Verify that the usage policies include a list of company-approved products.						
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	12.3.8.a Verify that the usage policies require automatic disconnect of sessions for remote-access technologies after a specific period of	Remote-access technologies are frequent "back doors" to critical resources and cardholder data. By disconnecting remote-access technologies when not in use (for example, those used to support your systems by your POS vendor, other vendors, or business partners), access and risk to networks is minimized.	YES				12.3.8: ssh remote sessions disconnect after period of inactivity from AWS console. For SKY access, the session does time out after 15 minute period of inactivity but is dependent the role of the individual accessing the system. 12.3.9: For vendors and businesses, we generally do not allow access to AWS via ssh or to SKY. Hence the no vendors have access answer still applies.
	12.3.8.b Examine configurations for remote access technologies to verify that remote access sessions will be automatically disconnected after a specific period of inactivity.						
12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use	12.3.9 Verify that the usage policies require activation of remote-access technologies used by vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.						
12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.	12.3.10.a Verify that the usage policies prohibit copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies.	To ensure all personnel are aware of their responsibilities to not store or copy cardholder data onto their local personal computers or other media, your policy should clearly prohibit such activities except for personnel that have been explicitly authorized to do so. Storing or copying cardholder data onto a local hard drive or other media must be in accordance with all applicable PCI DSS requirements.				YES	
	12.3.10.b For personnel with proper authorization, verify that usage policies require the protection of cardholder data in accordance with PCI DSS Requirements.						
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	12.4.a Verify that information security policies clearly define information security responsibilities for all personnel.	Without clearly defined security roles and responsibilities assigned, there could be inconsistent interaction with the security group, leading to unsecured implementation of technologies or use of outdated or unsecured technologies.	YES				GreenLots roles and responsbilities are being defined in Q1 2019.
	12.4.b Interview a sample of responsible personnel to verify they understand the security policies.						
12.4.1 Additional requirement for service providers only: Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: - Overall accountability for maintaining PCI DSS compliance - Defining a charter for a PCI DSS compliance program	12.4.1.a Examine documentation to verify executive management has assigned overall accountability for maintaining the entity's PCI DSS compliance.	Note: This requirement applies only when the entity being assessed is a service provider. Executive management assignment of PCI DSS compliance responsibilities ensures executive-level visibility into the PCI DSS compliance program and allows for the opportunity to ask appropriate questions to determine the effectiveness of the program and influence strategic priorities. Overall responsibility for the PCI DSS compliance program may be assigned to individual roles and/or to business units within the organization. Executive management may include C-level positions, board of directors, or	YES				
	12.4.1.b Examine the company's PCI DSS charter to verify it outlines the conditions under which the PCI DSS compliance program is organized and communicated to executive management.						
12.5 Assign to an individual or team the following information security management responsibilities:	12.5 Examine information security policies and procedures to verify: - The formal assignment of information security to a Chief Security Officer or other security-knowledgeable member of management. - The following information security responsibilities are specifically and formally assigned:	Each person or team with responsibilities for information security management should be clearly aware of their responsibilities and related tasks, through specific policy. Without this accountability, gaps in processes may open access into critical resources or cardholder data. Entities should also consider transition and/or succession plans for key personnel to avoid potential gaps in security assignments, which could result in responsibilities not being assigned and therefore not performed.					GreenLots Operations Team monitors and anlyzes alerts. They have been trained on policy and procedure.

12.5.1 Establish, document, and distribute security policies and procedures.	12.5.1 Verify that responsibility for establishing, documenting and distributing security policies and procedures is formally assigned.		YES				
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.	12.5.2 Verify that responsibility for monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel is formally assigned.						
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	12.5.3 Verify that responsibility for establishing, documenting, and distributing security incident response and escalation procedures is formally assigned.						
12.5.4 Administer user accounts, including additions, deletions, and modifications.	12.5.4 Verify that responsibility for administering (adding, deleting, and modifying) user account and authentication management is formally assigned.						
12.5.5 Monitor and control all access to data.	12.5.5 Verify that responsibility for monitoring and controlling all access to data is formally assigned.						
12.6 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security policy and procedures.	12.6.a Review the security awareness program to verify it provides awareness to all personnel about the importance of cardholder data security. 12.6.b Examine security awareness program procedures and documentation and perform the following:	If personnel are not educated about their security responsibilities, security safeguards and processes that have been implemented may become ineffective through errors or intentional actions.	YES				GreenLots HR and InfoSec Team have established and Information Security Awareness Training program.
12.6.1 Educate personnel upon hire and at least annually. *Note: Methods can vary depending on the role of the personnel and their level of access to the cardholder data.*	12.6.1.a Verify that the security awareness program provides multiple methods of communicating awareness and educating personnel (for example, posters, letters, memos, web-based training, meetings, and promotions). 12.6.1.b Verify that personnel attend security awareness training upon hire and at least annually. 12.6.1.c Interview a sample of personnel to verify they have completed awareness training and are aware of the importance of cardholder data security.	If the security awareness program does not include periodic refresher sessions, key security processes and procedures may be forgotten or bypassed, resulting in exposed critical resources and cardholder data.	YES				GreenLots new-hires, at least annually, receive Information Security Awareness training and updates.
12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	12.6.2 Verify that the security awareness program requires personnel to acknowledge, in writing or electronically, at least annually, that they have read and understand the information security policy.	Requiring an acknowledgement by personnel in writing or electronically helps ensure that they have read and understood the security policies/procedures, and that they have made and will continue to make a commitment to comply with these policies.	YES				
12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.) *Note: For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.*	12.7 Inquire with Human Resource department management and verify that background checks are conducted (within the constraints of local laws) prior to hire on potential personnel who will have access to cardholder data or the cardholder data environment.	Performing thorough background investigations prior to hiring potential personnel who are expected to be given access to cardholder data reduces the risk of unauthorized use of PANs and other cardholder data by individuals with questionable or criminal backgrounds.	YES				GreenLots employees are all background checked prior to offer letter being extended.

12.8 Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:	12.8 Through observation, review of policies and procedures, and review of supporting documentation, verify that processes are implemented to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data (for example, backup tape storage facilities, managed service providers such as web-hosting companies or security service providers, those that receive data for fraud modeling purposes, etc.), as follows:	If a merchant or service provider shares cardholder data with a service provider, certain requirements apply to ensure continued protection of this data will be enforced by such service providers. Some examples of the different types of service providers include backup tape storage facilities, managed service providers such as web-hosting companies or security service providers, entities that receive data for fraud-modeling purposes, etc.	YES				GreenLots reviews all policies and procedures annually or greater.
12.8.1 Maintain a list of service providers including a description of the service provided.	12.8.1 Verify that a list of service providers is maintained and includes a description of the service provided.	Keeping track of all service providers identifies where potential risk extends to outside of the organization.	YES				
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. *Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.*	12.8.2 Observe written agreements and confirm they include an acknowledgement by service providers that they are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.	The acknowledgement of the service providers evidences their commitment to maintaining proper security of cardholder data that it obtains from its clients. The extent to which the service provider is responsible for the security of cardholder data will depend on the particular service and the agreement between the provider and assessed entity. In conjunction with Requirement 12.9, this requirement is intended to promote a consistent level of understanding between parties about their applicable PCI DSS responsibilities. For example, the agreement may include the applicable PCI DSS requirements to be maintained as part of the provided service.	YES				GreenLots includes Data Privacy clause in contracts with third party service providers.
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	12.8.3 Verify that policies and procedures are documented and implemented including proper due diligence prior to engaging any service provider.	The process ensures that any engagement of a service provider is thoroughly vetted internally by an organization, which should include a risk analysis prior to establishing a formal relationship with the service provider. Specific due-diligence processes and goals will vary for each organization. Examples of considerations may include the provider's reporting practices, breach-notification and incident response procedures, details of how PCI DSS responsibilities are assigned between each party, how the provider validates their PCI DSS compliance and what evidence they will provide, etc.	YES				GreenLots has a Supplier Management Policy and Process.
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	12.8.4 Verify that the entity maintains a program to monitor its service providers' PCI DSS compliance status at least annually.	Knowing your service providers' PCI DSS compliance status provides assurance and awareness about whether they comply with the same requirements that your organization is subject to. If the service provider offers a variety of services, this requirement should apply to those services delivered to the client, and those services in scope for the client's PCI DSS assessment. The specific information an entity maintains will depend on the particular agreement with their providers, the type of service, etc. The intent is for the assessed entity to understand which PCI DSS requirements their providers have agreed to meet.	YES				GreenLots reviews each supplier, at least annually.
12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	12.8.5 Verify the entity maintains information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.						

12.9 Additional requirement for service providers only: Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment. *Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgement does not have to include the exact wording provided in this requirement.*	12.9 Additional testing procedure for service provider assessments only: Review service provider's policies and procedures and observe templates used for written agreements to confirm the service provider acknowledges in writing to customers that the service provider will maintain all applicable PCI DSS requirements to the extent the service provider possesses or otherwise stores, processes, or transmits cardholder data on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.	Note: This requirement applies only when the entity being assessed is a service provider. In conjunction with Requirement 12.8.2, this requirement is intended to promote a consistent level of understanding between service providers and their customers about their applicable PCI DSS responsibilities. The acknowledgement of the service providers evidences their commitment to maintaining proper security of cardholder data that it obtains from its clients. The service provider's internal policies and procedures related to their customer engagement process and any templates used for written agreements should include provision of an applicable PCI DSS acknowledgement to their customers. The method by which the service provider provides written acknowledgment should be agreed between the provider and their customers.	YES				Our mobile app handles payment information and never transmits it to our servers. The card data is never stored in full on our servers, and only a reference key (a unique identifier string unrelated to the payment card itself) is stored on our servers which is used to reference the payment card data which is stored securely on our 3rd party payment processor. We never store the full payment card number on our servers. We never store the payment card expiration date on our servers. We never store the authorization code otherwise known as the 'CVV' code on the back of the card on our servers. We never store the PIN of the payment card on our servers.
12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.	12.10 Examine the incident response plan and related procedures to verify entity is prepared to respond immediately to a system breach by performing the following:	Without a thorough security incident response plan that is properly disseminated, read, and understood by the parties responsible, confusion and lack of a unified response could create further downtime for the business, unnecessary public media exposure, as well as new legal liabilities.	YES				GreenLots has an Incident Response Policy and Plan.
12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: - Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum - Specific incident response procedures - Business recovery and continuity procedures - Data backup processes - Analysis of legal requirements for reporting compromises - Coverage and responses of all critical system components - Reference or inclusion of incident response procedures from the payment brands.	12.10.1.a Verify that the incident response plan includes: - Roles, responsibilities, and communication strategies in the event of a compromise including notification of the payment brands, at a minimum - Specific incident response procedures - Business recovery and continuity procedures - Data backup processes - Analysis of legal requirements for reporting compromises (for example, California Bill 1386, which requires notification of affected consumers in the event of an actual or suspected compromise for any business with California residents in their database) - Coverage and responses for all critical system components - Reference or inclusion of incident response procedures from the payment brands.	The incident response plan should be thorough and contain all the key elements to allow your company to respond effectively in the event of a breach that could impact cardholder data.	YES				
	12.10.1.b Interview personnel and review documentation from a sample of previously reported incidents or alerts to verify that the documented incident response plan and procedures were followed.						
12.10.2 Review and test the plan, including all elements listed in Requirement 12.10.1, at least annually.	12.10.2 Interview personnel and review documentation from testing to verify that the plan is tested at least annually, and that testing includes all elements listed in Requirement 12.10.1.	Without proper testing, key steps may be missed, which could result in increased exposure during an incident.	YES				GreenLots has not formally tested plan,but will do so in Q2 2019.
12.10.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	12.10.3 Verify through observation, review of policies, and interviews of responsible personnel that designated personnel are available for 24/7 incident response and monitoring coverage for any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts, and/or reports of unauthorized critical system or content file changes.	Without a trained and readily available incident response team, extended damage to the network could occur, and critical data and systems may become "polluted" by inappropriate handling of the targeted systems. This can hinder the success of a post-incident investigation.	YES				

12.10.4 Provide appropriate training to staff with security breach response responsibilities.	12.10.4 Verify through observation, review of policies, and interviews of responsible personnel that staff with responsibilities for security breach response are periodically trained.						
12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.	12.10.5 Verify through observation and review of processes that monitoring and responding to alerts from security monitoring systems, including detection of unauthorized wireless access points, are covered in the incident response plan.	These monitoring systems are designed to focus on potential risk to data, are critical in taking quick action to prevent a breach, and must be included in the incident-response processes.	YES				
12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	12.10.6 Verify through observation, review of policies, and interviews of responsible personnel that there is a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	Incorporating "lessons learned" into the incident response plan after an incident helps keep the plan current and able to react to emerging threats and security trends.	YES				
12.11 Additional requirement for service providers only: Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: - Daily log reviews - Firewall rule-set reviews - Applying configuration standards to new systems - Responding to security alerts - Change management processes *Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*	12.11.a Examine policies and procedures to verify that processes are defined for reviewing and confirming that personnel are following security policies and operational procedures, and that reviews cover: - Daily log reviews - Firewall rule-set reviews - Applying configuration standards to new systems - Responding to security alerts - Change management processes 12.11.b Interview responsible personnel and examine records of reviews to verify that reviews are performed at least quarterly.	Note: This requirement applies only when the entity being assessed is a service provider. Regularly confirming that security policies and procedures are being followed provides assurance that the expected controls are active and working as intended. The objective of these reviews is not to re-perform other PCI DSS requirements, but to confirm whether procedures are being followed as expected.	YES				GreenLots performs Quarterly Reviews.
12.11.1 Additional requirement for service providers only: Maintain documentation of quarterly review process to include: - Documenting results of the reviews - Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program *Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.*	12.11.1 Examine documentation from the quarterly reviews to verify they include: - Documenting results of the reviews - Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program	Note: This requirement applies only when the entity being assessed is a service provider. The intent of these independent checks is to confirm whether security activities are being performed on an ongoing basis. These reviews can also be used to verify that appropriate evidence is being maintained—for example, audit logs, vulnerability scan reports, firewall reviews, etc.—to assist the entity's preparation for its next PCI DSS assessment.	YES				

SCHEDULE D - APPENDIX 3
LETTER TEMPLATE

The following letter template shall be emailed by Supplier, to the City's PCI Office by sending an email to PCI.Compliance@Vancouver.ca on a calendar quarterly basis. Therefore, Supplier must provide a completed letter template in the form below, with required submissions attached, on March 30th, June 30th, September 30th, and December 30th of each calendar year for the duration of the Agreement. This letter template will be used to confirm that Supplier has met the following PCI-DSS requirements and has developed the appropriate evidence and documentation to support each of the listed requirements below.

Please note, the information set out in this template is for the purpose of confirming that Supplier has met the following calendar quarterly and annual requirements as requested by the City. There are still other PCI DSS obligations set out in the Agreement that Supplier is required to meet.

SENT BY E-MAIL

[DD/MM/YYYY]

Hello City of Vancouver PCI Office,

RE: Supply Agreement dated [insert date] between • ("Supplier") and City of Vancouver ("City") for the supply of electric vehicle charging goods and services (the "Agreement") - certain calendar quarterly and annual Supplier obligations under PCI Data Security Standards

Capitalized terms used in this letter will have the meaning given to them in the Agreement.

Supplier confirms that the following PCI-DSS requirements have been met for the following quarter, [QX] [YYYY], Supplier has developed the appropriate evidence and documentation to support each of the listed requirements, and the required submissions are attached to the e-mail.

If any of the following PCI-DSS requirements have not been met, detailed reasons are set out in an attachment to the e-mail.

Frequency of submission to the City	PCI-DSS Requirement	Submission Required by the City
Quarterly	Requirement 11.2. External Network Vulnerability Scan Report was performed by an Approved Scanning Vendor. These scans were performed with a passing result for Supplier on a quarterly basis.	Evidence of a passing scan.
Annually	Requirement 12.2. An annual risk assessment process is implemented that: • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal, documented analysis of risk This risk assessment is performed at least annually or upon significant changes to the environment.	Detailed Risk Assessment Report used to support PCI compliance.

SCHEDULE E – APPENDIX 1
ADDITIONAL PRIVACY AND DATA SECURITY REQUIREMENTS

Certain terms used in this document will have the meanings given below or in the Agreement. Supplier shall comply with the following terms and conditions relating to data security and compliance with applicable privacy legislation in respect of any Personal Information (as defined in section 1.1 below) acquired or accessed by Supplier in connection with the Agreement.

1.0 GENERAL

1.1 The following terms used in this document will have the following meanings:

(a) **"PIPA"** means the *Personal Information Protection Act* (British Columbia) as it may be amended or superseded from time to time;

(b) **"PIPEDA"** means the *Personal Information Protection and Electronic Documents Act* (Canada) as it may be amended or superseded from time to time; and

(c) "**Transmitted Data**" means all data or information, not including Personal Information, acquired, accessed or sent by the Supplier as a result of this Agreement, including all data or information acquired, accessed or sent by or through any software used by the Supplier to perform services under this Agreement, which data may include, without limitation, City proprietary or confidential information.

1.2 The Supplier shall not assign any of its rights or obligations under this document to a third party without the prior written consent of the City. If the City consents to the Supplier assigning certain of its rights or obligations to a third party, in addition to any other conditions the City may require, the Supplier shall ensure, and shall cause, its assignee to comply with the privacy and data security obligations set out in this document. Alternatively, in respect of complying with data security obligations hereunder, if the City consents to the Supplier using a third party to store the Transmitted Data (e.g. if the Supplier elects to use Infrastructure as a Service (Iaas) or Platform as a Service (Paas)), evidence satisfactory to the City that such third party is able to substantially comply with similar or a higher standard of data security than as set out in this document (e.g. ISO27001 SOC 2 Type II) shall be provided by the Supplier to the City.

2.0 PRIVACY AND DATA SECURITY

2.1 **Acknowledgment:** The Parties acknowledge that under this Agreement, Supplier will acquire or have access to Personal Information and that such Personal Information will not be acquired or accessed from, or provided by, the City. Supplier further acknowledges that it has obligations under, and will comply with Applicable Privacy Laws in respect of the collection, storage, use and protection of such Personal Information.

2.2 **Privacy Legislation and Obligations**

(a) Supplier confirms and acknowledges its obligations to comply with all Applicable Privacy Laws relating to privacy and Personal Information including PIPA and PIPEDA in relation to any Personal Information (as defined in such statutes) to which Supplier has access under this Agreement.

(b) Supplier has implemented appropriate or will implement appropriate policies and security measures to comply with all Applicable Privacy Laws, as well as to comply with the terms of this Agreement.

(c) Supplier agrees that all Personal Information to which Supplier has access under this Agreement is "under the control and custody" of the Supplier and the authority over the collection, use, disclosure, access, retention, destruction and integrity of all such information remains with the Supplier.

(d) Supplier agrees to collect, acquire, or hold only the minimum amount of Personal Information required to perform its duties under this Agreement. Unless otherwise authorized by Applicable Privacy Laws, Supplier must collect Personal Information directly from the individual to whom the information pertains.

(e) At or prior to the time of collection, Supplier must inform any person from whom it collects Personal Information:

2.2.e.1 The purpose for collecting it;

2.2.e.2 The legal authority for collecting it;

2.2.e.3 The title, business address and business telephone number of a person who can answer the individual's questions about the collection.

(f) All Transmitted Data (not including Personal Information) shall be treated as confidential and is supplied to Supplier only for the purpose of fulfilling the obligations under this Agreement. This obligation shall survive the expiry or termination of this Agreement. No such information shall be disclosed unless Supplier is legally compelled to do so and having first challenged that requirement and given the City an opportunity to challenge that requirement.

(g) Except with the prior written approval of or instructions from the City, Supplier shall not modify, add, delete, destroy, share, sell, match, mine, combine, manipulate or otherwise tamper with the Transmitted Data in any way.

(h) Supplier shall not withhold any Transmitted Data to enforce payment by the City or to enforce Supplier's rights in a dispute over this Agreement.

(i) As between the City and Supplier, the Transmitted Data are owned by the City, Supplier hereby agrees to hold such information in trust for the City, and Supplier makes no claim to any right of ownership in it.

2.3 **Authorized Purposes:** Supplier may only use the Transmitted Data to which Supplier has access under this Agreement to carry out Supplier's obligations under this Agreement and for no other purpose ("**Authorized Purposes**"). Any use or disclosure of such information by Supplier that is not expressly permitted by this Agreement will require the prior written consent of the City and must comply with all Applicable Laws.

2.4 **Restricted Access**

(a) Supplier will permit access to Transmitted Data only to those employees and authorized agents who need such access in order to carry out the Authorized Purposes (the "**Authorized Employees**"). Supplier will at all times maintain a current list of Authorized Employees. Supplier will, upon the City's request, provide the City with the list of Authorized Employees.

(b) Supplier will at all times have in place a knowledgeable senior person within its organization to be responsible for, or, to have the authority to ensure, compliance with the terms of this document (the "**Compliance Representative**"). The Compliance Representative will ensure that each Authorized Employee is aware of the terms of this

Agreement, and to maintain proof, in writing, that the terms have been explained and understood by each Authorized Employee. Upon entering into this Agreement, Supplier will notify the City in writing as to the name of the Supplier Compliance Representative. Supplier will promptly advise the City of any change to the Compliance Representative.

2.5 **Security:** Supplier will have appropriate physical, organizational and technological security measures (consistent with best practices in the software industry) in place to protect all Personal Information and Transmitted Data against accidental, unlawful, or unauthorized (i) destruction (ii) loss, (iii) alteration, (iv) disclosure, or (v) access (including remote access). Supplier will protect Personal Information against all other forms of unlawful processing including unnecessary collection, access, use, and disclosure beyond what is strictly necessary for the performance of the Agreement.

2.6 **Information Retention, Transfer to the City and Destruction:**

(a) **Supplier's Retention, Transfer to the City and Destruction:** Supplier is only permitted to retain Transmitted Data or any records of such information in any form whatsoever (including without limitation hard copy or electronic formats) during the term of this Agreement and for one year after the end of the term. During this period of time, Supplier shall hold all such information in compliance with the security and confidentiality requirements of this Agreement. At any time during the term of this Agreement and for a period of one year after the end of the term, Supplier shall, at the City's request, transfer a copy of any Transmitted Data to the City in a format reasonably requested by the City. Upon the expiry of one year after the end of the term, Supplier will transfer a copy of all Transmitted Data to the City in a format reasonably requested by the City and then permanently and securely destroy all such information and all records thereof in a manner that is appropriate for the media so all such information or any portion of it cannot be subsequently retrieved, accessed or used by Supplier or any other person. After all such information is transferred to the City and subsequently destroyed, Supplier shall deliver a written notice of confirmation to the City (in form and substance satisfactory to the City).

2.7 **Inspection and Compliance**

(a) During this Agreement and during the period of time that Supplier is permitted by this document to retain Personal Information and Transmitted Data, the City's authorized representative may, on reasonable notice and during regular business hours provide notice to Supplier and make reasonable inquiries about Transmitted Data in the possession of Supplier or any of Supplier's information management policies or practices relevant to its compliance with this Agreement.

(b) the City may request Supplier to provide a written certificate confirming Supplier's compliance with all obligations under this document, and if so requested, Supplier will within fifteen (15) Business Days provide to the City either:

2.7.b.1 such certificate; or

2.7.b.2 a notice of non-compliance with reasonable details in accordance with section 2.8.

(c) Supplier will, subject to Applicable Privacy Laws, promptly forward to the City any records that the City may request in order to review whether Supplier is complying with this Agreement.

(d) If requested by the City, acting reasonably, Supplier will appoint an independent, external auditor at the City's expense to review Supplier's information and security

practices under this Agreement. Supplier will provide copies of the results of any such audit to the City within seven (7) days of receiving the auditor's report.

(e) Supplier will promptly and fully comply with any investigation, review, order or ruling of the Office of the Information and Privacy Commissioner (British Columbia) in connection with the Personal Information and Transmitted Data.

2.8 **Written Notice of Non-Compliance.** Supplier will promptly notify the City in writing of any non-compliance or anticipated non-compliance with this document and will further inform the City of all steps Supplier proposes to take to address and prevent recurrence of such non-compliance or anticipated non-compliance.

2.9 **Survival:** The obligations in this document shall survive the expiration or earlier termination of this Agreement.

3.0 ADDITIONAL TERMS GOVERNING STORAGE AND ACCESS OF INFORMATION

3.1 Supplier shall, in respect of storage of, and access to and Transmitted Data**:**

(a) take a physical inventory, at least annually, of all records containing such information, to identify any losses;

(b) ensure that records are not removed from storage premises without appropriate written authorization from the City;

(c) use physically secure areas for the storage of records and restrict access to Authorized Employee;

(d) ensure that access to documentation about computer systems that contain such information is restricted to Authorized Employees;

(e) ensure that users of a system or network that processes such information are uniquely identified and that, before a user is given access to the system or such information, their identification is authenticated each time;

(f) implement procedures for identification and authentication, which include:

(i) controls for the issue, change, cancellation and audit-processing of user identifiers and authentication mechanisms;

(ii) ensuring that authentication codes or passwords:

(1) are generated, controlled and distributed so as to maintain the confidentiality and availability of the authentication code;

(2) are known only to the authorized user of the account;

(3) are pseudo-random in nature or vetted through a verification technique designed to counter triviality and repetition;

(4) are no fewer than 6 characters in length;

(5) are one-way encrypted;

(6) are excluded from unprotected automatic log-on processes; and

(7) are changed at irregular and frequent intervals at least semi-annually;

(g) maintain and implement formal procedures for terminated employees who have access to such information, with prompts to ensure revocation or retrieval of identity badges, keys, passwords and access rights;

(h) take reasonable security measures in respect of such information displayed on computer screens or in hardcopy form to prevent viewing or other access by unauthorized persons;

(i) implement automated or manual controls to prevent unauthorized copying, transmission or printing of such information; and

(j) implement control procedures to ensure the integrity of such information being stored, notably its accuracy and completeness.

3.2 Supplier must store Transmitted Data on agreed-upon media in accordance with prescribed techniques that store such information in a form that only Authorized Employees may access. These techniques may include translating such information into code (encryption) or shrinking or tightly packaging such information into unreadable form (compression).

3.3 Supplier shall store backup copies of Transmitted Data off-site under conditions which are the same as or better than originals.

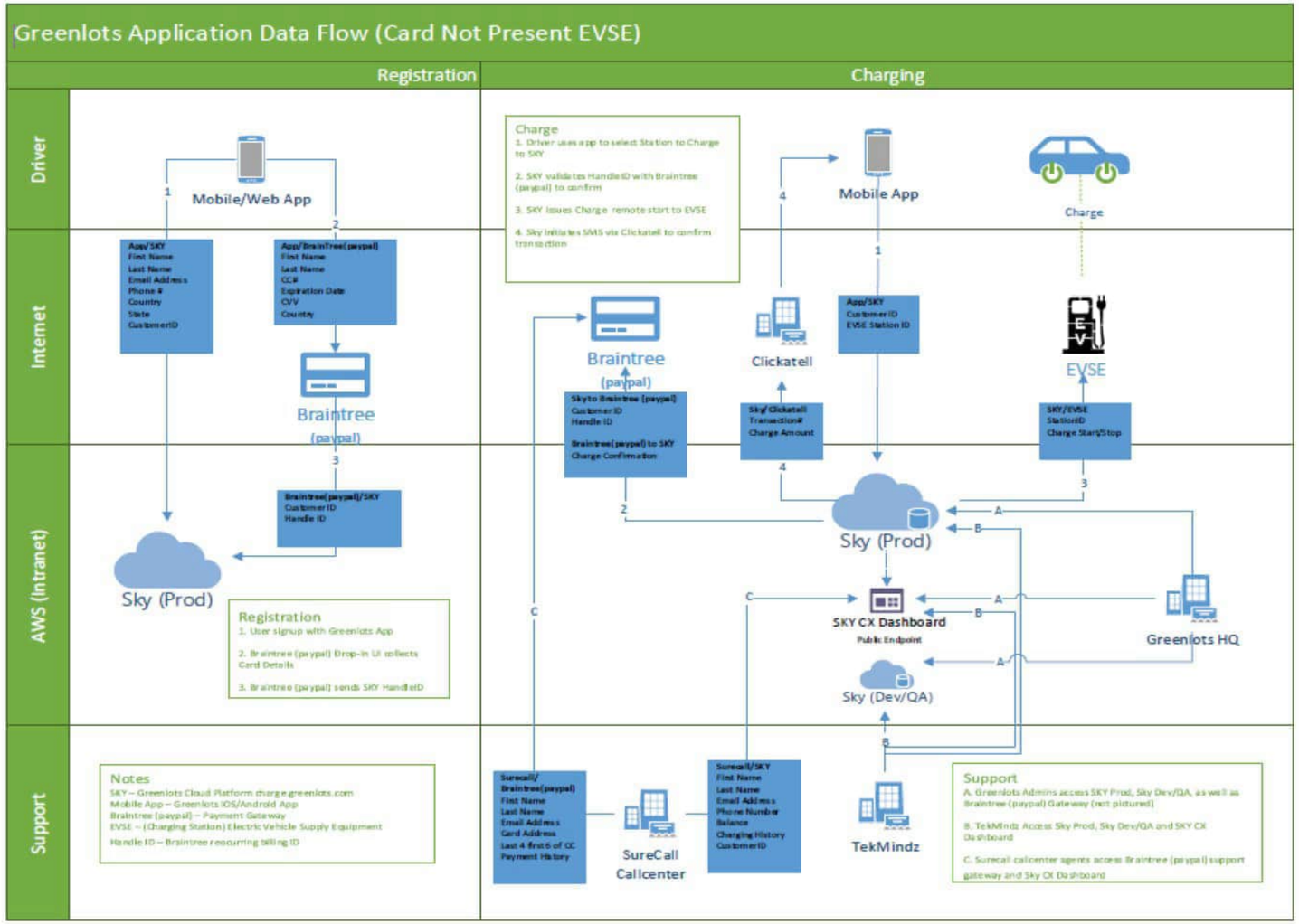
3.4 Supplier shall ensure the integrity of Transmitted Data stored, processed or transmitted through its system or network.

3.5 Supplier shall co-operate with, and assist in, any City investigation of a complaint or concern that Transmitted Data has been collected, used, handled, disclosed, stored, retained or destroyed contrary to the terms of this Agreement, or any other Applicable Laws.

SCHEDULE E - APPENDIX 2
PRIVACY REQUIREMENTS

Notes regarding this Appendix to Schedule E:

1) This document will be appended to Schedule E - Additional Privacy and Data Security Requirements of the Agreement. Supplier agrees that the content of this document is consistent with, and complies with, the terms and conditions of Schedule E.
2) Each capitalized term used in this document will have the meaning given to it in the Agreement except if it is defined in this document.
3) The term "personal information" used in this document has the meaning given to it in FOIPPA, PIPEDA and PIPA and the term "personal data" has the same meaning.

#	CITY OF VANCOUVER	GREENLOTS
1	Provide a detailed description, along with illustrative diagrams and flow charts, showing all data flows (e.g. the flow of data from when an EV user registers to use the City's EV network)	The Supplier will adhere to the following data flows: 

#	CITY OF VANCOUVER	GREENLOTS
2	What does the proponent use the data collected from EV users for?	The Supplier will: • Only use data collected in accordance with PIPA and/or PIPEDA and Supplier's privacy policy. • Not share personal data other than in accordance with PIPA and/or PIPEDA and Supplier's privacy policy, or with sub-contractors or service providers who have entered into agreements with Supplier and who are bound by terms and conditions substantially similar to those in the Agreement relating to the protection of privacy and personal information.
3	Does the proponent sell user data?	The Supplier will: • Not sell personal information obtained pursuant to the Agreement.
4	What is the proponent's privacy policy;	The Supplier will, continuously throughout the term of the Agreement, adhere to their privacy policy, currently published at: https://greenlots.com/privacy/ The Supplier covenants that its privacy policy will, continuously throughout the term of the Agreement, comply with the terms and conditions of the Agreement, and PIPA and/or PIPEDA.
5	Is EV user data stored on servers located in Canada?	The Supplier: • Currently stores EV user personal information in USA.
6	If user data is not stored in Canada, will your online or station user interface be able to obtain the consent of every user to having his/her data stored outside Canada?	The Supplier will: • Publish information in its privacy policy that personal data is stored outside Canada and may include storage in the United States or other countries.
7	Is the proponent able to provide the City with certain anonymous user data?	The Supplier will: • Provide anonymized charging station usage activity, trends and aggregated data.
8	Does the proponent have a good understanding of its obligations under PIPA and PIPEDA?	The Supplier: • Confirms a good understanding of its obligations under PIPA, and PIPEDA, and will fully comply with them.
9	Why does FOIPPA not apply to this Agreement?	The City and Supplier agree that FOIPPA does not apply to this Agreement on the basis of the following reasons: • All personal information collected by Supplier is collected through, and retained within, Supplier's or one or more subcontractors' software, • Supplier's software, and the software of its subcontractors, are not integrated with, or connected to, City software or hardware, • Supplier covenants that it will not disclose any personal information to the City, and • Based on the above, the City does not have custody or control, as such terms are used in, and as is required by, FOIPPA, of any personal information collected by Supplier. The City and Supplier agree that if any of the above reasons change during the term of this Agreement, the parties will, in good faith and acting reasonably, discuss any implications to Supplier's obligations in respect of the collection, storage, use and protection of personal information including Supplier's obligations in respect of data security and whether Supplier may need to comply with FOIPPA at such time. If at such time Supplier is required to comply with FOIPPA, Supplier will use commercially reasonable efforts to do so. Supplier acknowledges and agrees that Supplier's collection, storage, use and protection of personal information in accordance with all applicable Laws including, without limitation, FOIPPA (if applicable), is a material condition of this Agreement and, as a result, if the City is not satisfied, acting reasonably, that Supplier is able to comply with FOIPPA, the City may, at its option, terminate the Agreement in accordance with Section 12.2 of the Agreement. If the City terminates the Agreement in accordance with Section 12 of the Agreement, the City's sole liability to Supplier will be the amounts payable to Supplier for services performed in accordance with the Agreement through the date of termination.

SCHEDULE F -
TECHNOLOGY REQUIREMENTS

#	FUNCTION	CITY OF VANCOUVER	GREENLOTS
1	**Application Architecture**	The Supplier must provide the following: • Application is built using .Net or Java. • Server components and databases are built into the application. • Configurational metadata storage. • SMTP supported email notifications. • Future versions of the applications must be compatible with earlier versions.	The Supplier will provide SKY Deployment application software, which is: • Java enterprise edition. • A Cloud-hosted system that leverage multiple server-based components. • SKY uses MySQL RDBMS and ElasticSearch. • Configuration metadata is stored in relational database. • SMTP is supported for email notification. • Future versions of the application are backwards compatible with earlier ones.
2	**Deployment Architecture**	The Supplier must provide the following: • An application that is compatible and can be hosted in a Cloud environment hosted in a Canadian data centre. • Defined RTO (recovery time objective) of 2 hours. • Defined RPO (recovery point objective) of 24 hours. • Controls to keep the City's services and data logically separate from other customers that use the Suppliers application. • Confirmation that the City's data will be backed up, archived and deleted from the system when needed. • A completed Cloud Security Alliance questionnaire.	The Supplier will provide: • Cloud-hosted application using AWS. The SKY application leverages the following: a) Greenlots o HQ - Los Angeles, CA o SKY production server location - AWS California o SKY development server location - AWS California b) Braintree/PayPal (payment processor) o HQ - San Jose, CA o Server location will not be divulged by PayPal/BT. c) Clickatell (SMS) o HQ - Redwood City, CA. o Server location not be divulged by Clickatell. d) Tekmindz o HQ - Noida, India. o Servers location - NA, they use GL servers. e) SureCall o HQ - Calgary, Canada o Servers location - TBD • RTO is 1-2 hours. • RPO is 24 hours, with daily data backups. • The City of Vancouver's services will be deployed with other Greenlots' customers and will not be kept separate from other Greenlots customers. • Greenlots is using multi-tenant SaaS solution. A dedicated hosting option is not being used for COV. • The City of Vancouver's data will be backed up, archived, and deleted from the system when need. • Cloud Security Alliance Questionnaire completed on June 12, 2019 (attached).

#	FUNCTION	CITY OF VANCOUVER	GREENLOTS
3	Availability and Scalability	The Supplier must provide the following: • The application will support 24x7 availability with 99.99% uptime. • There will be no limit on the number of registered users the package can support. • There will be no maximum limit to the amount of transactions, collaborations, events being managed (workflow) that can be handled per session, per day. • The average response time for initial page load, page access, and database access will be 15 seconds. • The application will maintain transaction and data integrity in failure situations. • The application will maintain transaction logs. • The application will leverage caching techniques for loading pages, static content and data. All administration activities can be performed with the application up and running in production.	The Supplier will provide: • 3 tiered with distributed caching and queuing along with micro services architecture to support 24x7 availability with 99.99% uptime and transparent failover protection. • There is no limit on the number of registered users the package can support. • There is no maximum limit to the amount of transactions, collaborations, events being managed (workflow) that can be handled per session, per day. • The average response time for initial page load, page access, and database access is 15 seconds. • Application maintains transaction and data integrity in failure situations. • Commit of data only occurs on success, otherwise it is a rollback and appropriate error is returned to client calling the services. • AWS RDS (Amazon Relational Database Service) used for scale and failure. • Application maintains transaction logs. • Application uses Redis and Elastic Server for loading pages, static content, data, etc. • All administration activities can be performed with the application up and running in production.
4	User Interface Standards	The Supplier must provide the following: • The application will provide a website for drivers and City staff, as well as driver-facing iOS and Android apps. • The web application will be available as a responsive web, not requiring download or install by end user. • The web application will be responsive by design (HTML5, supports mobile and various screen sizes). The web based application and mobile apps will comply with the City's Digital Style Guidelines (https://company-66050.frontify.com/d/3vgsw7ZF6Ppb).	The Supplier will provide: • A driver-facing app on iOS and Android, and • A web site that is available as a responsive web, not requiring download or install by end user. • A web-based application responsive by design. • A web-based application that offers the ability to white-label the mobile apps and web portals to comply with the City's Digital Style Guidelines. • Note: although Greenlots can work with the City to scope and develop a white-label solution, the web application used for this program is the Greenlots platform and is not a white-label product. A white-label application is not in our existing scope and is not reflected in our software licensing or project pricing.
5	Security	The Supplier must provide the following: • A user ID and password will be used by both drivers and City of Vancouver staff to access the application. • Password history should be maintained to prevent users from recycling passwords. • The application should enable the City or the vendor to force users to change their passwords periodically. • The application should prompt the user for a new password when the current password is nearing expiration. • The password minimum length should be configured to a minimum of 10 characters • Idle users will be required to re login. • Security managed at a group level and the access controls are defined by roles. • Application to track at a minimum a user's last login time. • HTTPS will be supported at a minimum of TLS1.2. • Form level validation will be provided by the application. • Format level validation will be provided by the application. • Content validation will be provided by the application. • SIEM will be provided by the application.	The Supplier will provide: • Staff and citizen will access the application with a user ID and password. • Application currently has the following features: o Configure the password minimum length. For SKY Admin users, minimum password length is currently set at 10 characters. For Drivers, minimum password length is currently set at 8 characters. All password lengths are configurable at a global level. o Require idle users to log back in. o Support the HTTPS protocol. o Form level validation, format validation, and content validation. o SIEM. o Track last login time. This information can be made available to the City of Vancouver as requested. o Manage the security at a group level, and the access controls defined by roles • Application complies with all Privacy legislation applicable to the data under consideration: a) BC's Personal Information Protection Act, SBC 2003 c. 36 b) Federal Personal Information Protection and Electronic Documents Act, SC 2000 c 5 c) Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165 (FIPPA)

#	FUNCTION	CITY OF VANCOUVER	GREENLOTS
		• A third party should complete penetration tests every year and the results shared with the City of Vancouver. • The application will comply with all Privacy legislation applicable to the data under consideration: a) BC's Personal Information Protection Act, SBC 2003 c. 36 b) Federal Personal Information Protection and Electronic Documents Act, SC 2000 c 5 c) Freedom of Information and Protection of Privacy Act, RSBC 1996, c 165 (FIPPA)	• Future roadmap items to be completed by the Supplier in 2022: o Password history is maintained to prevent users from recycling passwords. o Enable the City of Vancouver or the vendor to force users to change their passwords periodically. o Prompt the user for a new password when the current password is nearing expiration. o Lock out of users after a number of failed login attempts. o Provide SSO with the City's authentication. Multi-Factor Authentication (MFA).
6	Integration	The Supplier must provide the following: • The application will support SOAP and REST/JSON web services. • All application data is available from the Web Services. • There will be access or authorization control for all Web Services, including credential based. • The web services will be extensible through publically documented APIs. • The application can support integration via file transfers, including CSV format via sFTP The application will support the manual export of search results or report data in the following file formats: XML, HTML, and Excel/CSV.	The Supplier will provide: • Application supports Web Services via REST/JSON based on the service. • Certain application data is available from Web Services listed above. • Access or authorization control of these Web Services available. Different APIs employ different authentication approaches, but general authentication is credential based. • Application uses open standard API's that are easily developed by clients. Additionally, application uses adaptor pattern where needed for customization and flexibility. • Integrations via file transfers is supported. CSV via sftp for batch transfers. • Application supports export of search results or report data in the following file formats: CSV.
7	Data and Reporting	The Supplier must provide the following: • The City of Vancouver will remain the sole owner of all data entered, used, and maintained within the application. The vendor will not share the data in its native format with third parties. • The application will support out-of-the-box reporting. • The City of Vancouver will have self-service access to the application's out-of-the-box reporting. • All of the City's application data can be extracted fully to the City for use in internal analytics or other purposes. • The application will make available via API details on charging station locations (and attributes) for use in the City's other channels (open data, etc.).	The Supplier confirms: • The City will retain independent rights to use all charging data (defined below) maintained within the application. The vendor will not share the charging data in its native format with third parties. The only use of charging data is for research and system performance and enhancement purposes and it is not shared in its native format with third parties. • Driver data (defined below) is owned by the Supplier. • Application provides out-of-the-box reports. • The City of Vancouver will have self-service access to the applications reports. • For specific, agreed upon scenarios, application data can be fully extracted for the City of Vancouver's use in internal reporting software. A read only copy of the database can be provided. Scope and cost for such data extraction would need to be discussed and agreed upon. • Routine data extraction would need to occur via APIs or CSV batch file transfer. • Charging station location data is available via OCPI API. • The term "charging data" means anonymous or aggregated charge station performance/operational data and excludes driver data (defined below) • The term "driver data" means the personal and financial information of drivers who use the charge stations
8	Network	The Supplier must provide the following: • Deployed components will use LTE connectivity provided by the vendor with connection to the vendor's cloud application.	The Supplier will provide: • Both cellular and WIFI connections depending on the installation as follows: o Each charging station has its own onboard modem and cellular SIM card. o Depending on the SKU, certain charging stations can be configured in a satellite/hub configuration.

SCHEDULE F – APPENDIX 1
TECHNOLOGY - CAIQ

Excel file with three (3) tabs

Note: the Excel file is provided as an attachment in this electronic executed PDF copy of the Agreement.

CAIQv3.0.1 CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1

Control Domain	Control ID	Question ID	Control Specification	Consensus Assessment Questions	Consensus Assessment Answers			Notes	ISO/IEC 27001:2013
					Yes	No	N/A		
Application & Interface Security *Application Security*	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.	Do you use industry standards (Build Security in Maturity Model [BSIMM] benchmarks, Open Group ACS Trusted Technology Provider Framework, NIST, etc.) to build in security for your Systems/Software Development Lifecycle (SDLC)?	YES			OWASP Top 10 is followed for secure development of application. ISO 4/15/19	A9.4.2 A9.4.1, 8.1*Partial, A14.2.3, 8.1*partial, A.14.2.7
		AIS-01.2		Do you use an automated source code analysis tool to detect security defects in code prior to production?	YES			OWASP Top 10 is followed for secure development of application. ISO 4/15/19	A12.6.1, A18.2.2
		AIS-01.3		Do you use manual source-code analysis to detect security defects in code prior to production?	YES			OWASP Top 10 is followed for secure development of application. (ISO 4/15/19)	
		AIS-01.4		Do you verify that all of your software suppliers adhere to industry standards for Systems/Software Development Lifecycle (SDLC) security?	YES			OWASP Top 10 is followed for secure development of application. (ISO 4/15/19)	
		AIS-01.5		(SaaS only) Do you review your applications for security vulnerabilities and address any issues prior to deployment to production?	YES			OWASP Top 10 is followed for secure development of application. (ISO 4/15/19)	
Application & Interface Security *Customer Access Requirements*	AIS-02	AIS-02.1	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	Are all identified security, contractual, and regulatory requirements for customer access contractually addressed and remediated prior to granting customers access to data, assets, and	YES			Access Control Policy is in place. (ISO 4/15/19)	A9.1.1.
		AIS- 02.2		Are all requirements and trust levels for customers' access defined and documented?	YES			Access Control Policy is in place. (ISO 4/15/19)	
Application & Interface Security *Data Integrity*	AIS-03	AIS-03.1	Data input and output integrity routines (i.e., reconciliation and edit checks) shall be implemented for application interfaces and databases to prevent manual or systematic processing errors, corruption of data, or misuse.	Are data input and output integrity routines (i.e., reconciliation and edit checks) implemented for application interfaces and databases to prevent manual or systematic processing errors or corruption of data?	PARTIAL			Access Control, and Cryptographic Control, and Privacy policies are in place. All information sharing channels are protected with encryption or restrictions on type of data shared, however, there is no formal data transfer policy or procedure. (ISO 4/15/19)	A13.2.1, A13.2.2, A9.1.1, A9.4.1, A10.1.1 A18.1.4
Application & Interface Security *Data Security / Integrity*	AIS-04	AIS-04.1	Policies and procedures shall be established and maintained in support of data security to include (confidentiality, integrity, and availability) across multiple system interfaces, jurisdictions, and business functions to prevent improper disclosure, alternation, or destruction.	Is your Data Security Architecture designed using an industry standard (e.g., CDSA, MULITSAFE, CSA Trusted Cloud Architectural Standard, FedRAMP, CAESARS)?	PARTIAL			Access Control, and Cryptographic Control, and Privacy policies are in place. All information sharing channels are protected with encryption or restrictions on type of data shared, however, there is no formal data transfer policy or procedure. (ISO 4/15/19)	A13.2.1, A13.2.2, A9.1.1, A9.4.1, A10.1.1 A18.1.4

Audit Assurance & Compliance *Audit Planning*	AAC-01	AAC-01.1	Audit plans shall be developed and maintained to address business process disruptions. Auditing plans shall focus on reviewing the effectiveness of the implementation of security operations. All audit activities must be agreed upon prior to executing any audits.	Do you produce audit assertions using a structured, industry accepted format (e.g., CloudAudit/A6 URI Ontology, CloudTrust, SCAP/CYBEX, GRC XML, ISACA's Cloud Computing Management Audit/Assurance Program, etc.)?	YES			Audit Roadmap is planned and can be made available.	Clauses 4.3(a), 4.3(b), 5.1(e), 5.1(f), 6.2(e), 9.1, 9.1(e), 9.2, 9.3(f), A12.7.1
Audit Assurance & Compliance *Independent Audits*	AAC-02	AAC-02.1	Independent reviews and assessments shall be performed at least annually to ensure that the organization addresses nonconformities of established policies, standards, procedures, and compliance obligations.	Do you allow tenants to view your SOC2/ISO 27001 or similar third-party audit or certification reports?	YES			The ISMS Policy is in place. (ISO 4/15/19)	Clauses 4.3(a), 4.3(b), 5.1(e), 5.1(f), 9.1, 9.2, 9.3(f), A18.2.1
		AAC-02.2		Do you conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices	YES			The ISMS Policy is in place. (ISO 4/15/19)	
		AAC-02.3		Do you conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices	YES			The ISMS Policy is in place. (ISO 4/15/19)	
		AAC-02.4		Do you conduct internal audits regularly as prescribed by industry best practices and guidance?	YES			The ISMS Policy is in place. (ISO 4/15/19)	
		AAC-02.5		Do you conduct external audits regularly as prescribed by industry best practices and guidance?	YES			The ISMS Policy is in place. (ISO 4/15/19)	
		AAC-02.6		Are the results of the penetration tests available to tenants at their request?	YES			The ISMS Policy is in place. (ISO 4/15/19)	
		AAC-02.7		Are the results of internal and external audits available to tenants at their request?	YES			The ISMS Policy is in place. (ISO 4/15/19)	
		AAC-02.8		Do you have an internal audit program that allows for cross-functional audit of assessments?	YES			The ISMS Policy is in place. (ISO 4/15/19)	
Audit Assurance & Compliance *Information System Regulatory Mapping*	AAC-03	AAC-03.1	Organizations shall create and maintain a control framework which captures standards, regulatory, legal, and statutory requirements relevant for their business needs. The control framework shall be reviewed at least annually to ensure changes that could affect the business processes are reflected.	Do you have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data?	Yes			all relevant legal information security requirements for the organization and information systems have been identified. Currently following ISO Framework (ISO 4/15/19)	Clauses 4.2(b), 4.4, 5.2(c), 5.3(ab), 6.1.2, 6.1.3, 6.1.3(b), 7.5.3(b), 7.5.3(d), 8.1, 8.3 9.2(g), 9.3, 9.3(b), 9.3(f), 10.2, A.8.2.1, A.18.1.1, A.18.1.3, A.18.1.4, A.18.1.5
		AAC-03.2		Do you have the capability to recover data for a specific customer in the case of a failure or data loss?	Yes			all relevant legal information security requirements for the organization and information systems have been identified. Currently following ISO Framework (ISO 4/15/19)	
		AAC-03.3		Do you have the capability to restrict the storage of customer data to specific countries or geographic locations?	Yes			all relevant legal information security requirements for the organization and information systems have been identified. Currently following ISO Framework (ISO 4/15/19)	
		AAC-03.4		Do you have a program in place that includes the ability to monitor changes to the regulatory requirements in relevant jurisdictions, adjust your security program for changes to legal requirements, and ensure compliance with relevant regulatory requirements?	Yes			all relevant legal information security requirements for the organization and information systems have been identified. Currently following ISO Framework (ISO 4/15/19)	

Business Continuity Management & Operational Resilience *Business Continuity Planning*	BCR-01	BCR-01.1	A consistent unified framework for business continuity planning and plan development shall be established, documented, and adopted to ensure all business continuity plans are consistent in addressing priorities for testing, maintenance, and information security requirements. Requirements for business continuity plans include the following: • Defined purpose and scope, aligned with relevant dependencies • Accessible to and understood by those who will use them • Owned by a named person(s) who is responsible for their review, update, and approval • Defined lines of communication, roles, and responsibilities • Detailed recovery procedures, manual work-around, and reference information • Method for plan invocation	Do you provide tenants with geographically resilient hosting options?	YES			Data centers are located across multiple geographic zones to ensure resiliency. (ISO 4/15/19)	Clause 5.1(h) A.17.1.2
		BCR-01.2		Do you provide tenants with infrastructure service failover capability to other providers?	YES			Data centers are located across multiple geographic zones to ensure service failover capability. Other systems rely on the BCP plan of the provider to ensure continuity in case of failure. (ISO 4/15/19)	
Business Continuity Management & Operational Resilience *Business Continuity Testing*	BCR-02	BCR-02.1	Business continuity and security incident response plans shall be subject to testing at planned intervals or upon significant organizational or environmental changes. Incident response plans shall involve impacted customers (tenant) and other business relationships that represent critical intra-supply chain business process dependencies.	Are business continuity plans subject to testing at planned intervals or upon significant organizational or environmental changes to ensure continuing effectiveness?	Partial			BCP exists, but has not fully been implemented. Table Top Exercises occur on an annual basis.	A17.3.1
Business Continuity Management & Operational Resilience *Power / Telecommunications*	BCR-03	BCR-03.1	Data center utilities services and environmental conditions (e.g., water, power, temperature and humidity controls, telecommunications, and internet connectivity) shall be secured, monitored, maintained, and tested for continual effectiveness at planned intervals to ensure protection from unauthorized interception or damage, and designed with automated fail-over or other redundancies in the event of planned or unplanned disruptions.	Do you provide tenants with documentation showing the transport route of their data between your systems?	YES			Power and telecommunication cables are managed by the LA, India and Monrovia facilities site provider; a review has taken place. (ISO 4/15/19)	A11.2.2, A11.2.3
		BCR-03.2		Can tenants define how their data is transported and through which legal jurisdictions?	YES			Power and telecommunication cables are managed by the WeWork site provider; a review has taken place. (ISO 4/15/19)	

Business Continuity Management & Operational Resilience Documentation	BCR-04	BCR-04.1	Information system documentation (e.g., administrator and user guides, and architecture diagrams) shall be made available to authorized personnel to ensure the following: • Configuring, installing, and operating the information system • Effectively using the system's security features	Are information system documents (e.g., administrator and user guides, architecture diagrams, etc.) made available to authorized personnel to ensure configuration, installation and operation of the information system?	Partial			Greenlots has documented operating policies and some procedures for backups, equipment maintenance, Media handling, mail handling and management safety etc. (ISO 4/15/19)	Clause 9.2(g)
Business Continuity Management & Operational Resilience *Environmental Risks*	BCR-05	BCR-05.1	Physical protection against damage from natural causes and disasters, as well as deliberate attacks, including fire, flood, atmospheric electrical discharge, solar induced geomagnetic storm, wind, earthquake, tsunami, explosion, nuclear accident, volcanic activity, biological hazard, civil unrest, mudslide, tectonic activity, and other forms of natural or man-made disaster shall be anticipated, designed, and have countermeasures applied.	Is physical protection against damage (e.g., natural causes, natural disasters, deliberate attacks) anticipated and designed with countermeasures applied?	YES			The Physical Security Policy and supporting procedure is in place to ensure protection and recovery in the case of environmental damage. Additionally, sites are located in geographically diverse locations to ensure backups will be available. (ISO 4/15/19)	A11.1.4, A11.2.1
Business Continuity Management & Operational Resilience *Equipment Location*	BCR-06	BCR-06.1	To reduce the risks from environmental threats, hazards, and opportunities for unauthorized access, equipment shall be kept away from locations subject to high probability environmental risks and supplemented by redundant equipment located at a reasonable distance.	Are any of your data centers located in places that have a high probability/occurrence of high-impact environmental risks (floods, tornadoes, earthquakes, hurricanes, etc.)?	YES			The Physical Security Policy and supporting procedure is in place to ensure protection and recovery in the case of environmental damage. Additionally, sites are located in geographically diverse locations to ensure backups will be available. (ISO 4/15/19)	A11.2.1
Business Continuity Management & Operational Resilience *Equipment Maintenance*	BCR-07	BCR-07.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for equipment maintenance ensuring continuity and availability of operations and support personnel.	If using virtual infrastructure, does your cloud solution include independent hardware restore and recovery capabilities?	YES			All virtual infrastructure security measures are inherited from AWS. (ISO 4/15/19)	A11.2.4
		BCR-07.2		If using virtual infrastructure, do you provide tenants with a capability to restore a Virtual Machine to a previous state in time?	YES			All virtual infrastructure security measures are inherited from AWS. (ISO 4/15/19)	

		BCR-07.3		If using virtual infrastructure, do you allow virtual machine images to be downloaded and ported to a new cloud provider?	YES			All virtual infrastructure security measures are inherited from AWS. (ISO 4/15/19)	
		BCR-07.4		If using virtual infrastructure, are machine images made available to the customer in a way that would allow the customer to replicate those images in their own off-site storage location?	YES			All virtual infrastructure security measures are inherited from AWS. (ISO 4/15/19)	
		BCR-07.5		Does your cloud solution include software/provider independent restore and recovery capabilities?	YES			All virtual infrastructure security measures are inherited from AWS. (ISO 4/15/19)	
Business Continuity Management & Operational Resilience *Equipment Power Failures*	BCR-08	BCR-08.1	Protection measures shall be put into place to react to natural and man-made threats based upon a geographically-specific business impact assessment.	Are security mechanisms and redundancies implemented to protect equipment from utility service outages (e.g., power failures, network disruptions, etc.)?	YES			The Physical Security Policy and supporting procedure is in place the ensure protection in the case of a power failure or service outage. (ISO 4/15/19)	A.11.2.2, A.11.2.3, A.11.2.4
Business Continuity Management & Operational Resilience *Impact Analysis*	BCR-09	BCR-09.1	There shall be a defined and documented method for determining the impact of any disruption to the organization (cloud provider, cloud consumer) that must incorporate the following: • Identify critical products and services • Identify all dependencies, including processes, applications, business partners, and third party service providers • Understand threats to critical products and services • Determine impacts resulting from planned or unplanned disruptions and how these vary over time • Establish the maximum tolerable period for disruption • Establish priorities for recovery • Establish recovery time objectives for resumption of critical products and services within their maximum tolerable period of disruption • Estimate the resources required for resumption	Do you provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance?	PARTIAL			BCP Policy exists, however is not being formally implemented or enforced. (ISO 4/15/19) -Scheduled for 10/01/2019	A.17.1.1 A.17.1.2
		BCR-09.2		Do you make standards-based information security metrics (CSA, CAMM, etc.) available to your tenants?	PARTIAL			BCP Policy exists, however is not being formally implemented or enforced. (ISO 4/15/19) -Scheduled for 10/01/2019	
		BCR-09.3		Do you provide customers with ongoing visibility and reporting of your SLA performance?	PARTIAL			BCP Policy exists, however is not being formally implemented or enforced. (ISO 4/15/19) -Scheduled for 10/01/2019	
Business Continuity Management & Operational Resilience *Policy*	BCR-10	BCR-10.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for appropriate IT governance and service management to ensure appropriate planning, delivery and support of the organization's IT capabilities supporting business functions, workforce, and/or customers based on industry acceptable standards (i.e., ITIL v4 and COBIT 5). Additionally, policies and procedures shall include defined roles and responsibilities supported by regular workforce training.	Are policies and procedures established and made available for all personnel to adequately support services operations' roles?	YES			A Roles & Responsibilities matrix is in place, which includes job descriptions and security duties. The Information Security Policy, which will outline expectations and responsibilities for all personnel, is currently in draft stage. (ISO 4/15/19)	Clause 5.1(h) A.6.1.1 A.7.2.1 A.7.2.2 A.12.1.1
Business Continuity Management & Operational Resilience *Retention Policy*	BCR-11	BCR-11.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, for defining and adhering to the retention period of any critical asset as per established policies and procedures, as well as applicable legal, statutory, or regulatory compliance obligations. Backup and recovery measures shall be incorporated as part of business continuity planning and tested accordingly for effectiveness.	Do you have technical control capabilities to enforce tenant data retention policies?	YES			Backups are confirmed in AWS to EC 2 daily. All other services utilitzed are cloud-based and therefore backup themselves. All back-up local data is shared with "Crash_Plan". (ISO 4/15/19)	Clauses 9.2(g) 7.5.3(b) 5.2 (c) 7.5.3(d) 5.3(a) 5.3(b) 8.1 8.3 A.12.3.1

		BCR-11.2		Do you have a documented procedure for responding to requests for tenant data from governments or third parties?	YES			Backups are confirmed in AWS to EC 2 daily. All other services utilitzed are cloud-based and therefore backup themselves. All back-up local data is shared with "Crash_Plan". (ISO 4/15/19)	A.8.2.3
		BCR-11.4		Have you implemented backup or redundancy mechanisms to ensure compliance with regulatory, statutory, contractual or business requirements?	YES			Backups are confirmed in AWS to EC 2 daily. All other services utilitzed are cloud-based and therefore backup themselves. All back-up local data is shared with "Crash_Plan". (ISO 4/15/19)	
		BCR-11.5		Do you test your backup or redundancy mechanisms at least annually?	YES			Backups are confirmed in AWS to EC 2 daily. All other services utilitzed are cloud-based and therefore backup themselves. All back-up local data is shared with "Crash_Plan". (ISO 4/15/19)	
Change Control & Configuration Management *New Development / Acquisition*	CCC-01	CCC-01.1	Policies and procedures shall be established, and supporting business processes and technical measures implemented, to ensure the development and/or acquisition of new data, physical or virtual applications, infrastructure network and systems components, or any corporate, operations and/or data center facilities have been pre-authorized by the organization's business leadership or other accountable business role or function.	Are policies and procedures established for management authorization for development or acquisition of new applications, systems, databases, infrastructure, services, operations and facilities?	YES			Security requirements have been identified for the product SKY. The ISMS Policy is in place. (ISO 4/15/19)	A.14.1.1 A.12.5.1 A.14.3.1 A.9.4.5 8.1* (partial) A.14.2.7 A.18.1.3 A.18.1.4
		CCC-01.2		Is documentation available that describes the installation, configuration, and use of products/services/features?	YES			Security requirements have been identified for the product SKY. The ISMS Policy is in place. (ISO 4/15/19)	
Change Control & Configuration Management *Outsourced Development*	CCC-02	CCC-02.1	External business partners shall adhere to the same policies and procedures for change management, release, and testing as internal developers within the organization (e.g., ITIL service management processes).	Do you have controls in place to ensure that standards of quality are being met for all software development?	PARTIAL			Information security agreements with external partners are currently in draft with Greenlots' Legal department. (ISO 4/15/19)	A18.2.1 A.15.1.2 A.12.1.4 8.1* (partial) 8.1* (partial) A.15.2.1 8.1* (partial) A.15.2.2 A.14.2.9