City of Coquitlam
Terms and Conditions of Purchase
Payment Card Industry (PCI) Data Security Standard (DSS)

1. Application

If, through the supply of goods or services, the Vendor will have access to or the ability to impact the City's information technology environment, will receive, possess, store, process or transmit payment cardholder data on behalf of the City or using the City's information technology, or will provide software, equipment or systems that the City will use or allow to be used to process cardholder data, the Vendor agrees to comply with and be bound by the provisions set out herein.

2. PCI DSS Applicable Goods and Services

If the Vendor is supplying goods or services that support the City's payment card environment, including payment applications, services and products (e.g., PIN Transaction Security devices), or security products and services that support the City's information technology environment, and where such goods or services are required under the Payment Card Industry Data Security Standard ("PCI DSS") to be PCI DSS, PA-DSS or PCI PTS (or similar standard) compliant, the Vendor will provide, prior to delivery of the goods or services, and on an annual basis thereafter, a PCI DSS Attestation of Compliance ("AOC") signed by a third-party Qualified Security Assessor ("QSA") or qualified Internal Security Assessor (ISA) and a Report on Compliance ("RoC") with the relevant sections of the ROC supporting the product and services being provided and with confidential information redacted where sensitive information can be reviewed when required. With the prior written consent of the City, the Vendor may provide a QSA letter on QSA company letterhead that discusses the controls and services provided by the Vendor in lieu of an RoC.

If the City determines that a Vendor has not satisfied the supporting control documentation requirements set out in this section 2 or the products and services have not been sufficiently tested, the Vendor will allow the City (or its designated third party assessor) to review on at least an annual basis, those product and service controls consistent with the relevant PCI DSS standards that will enable the City to fulfill its own PCI DSS obligations.

If the Vendor fails to maintain at any time its PCI DSS compliance (or other relevant standards), the Vendor must notify the City within 30 days of such failure and the City may elect to terminate the agreement upon written notice to the Vendor.

3. Access Controls

In the event a Vendor is provided internet access by the City, or the Vendor otherwise has access to the City's information security assets, the Vendor acknowledges and agrees that such access is provided on an individual basis, may not be shared and will terminate upon completion, expiry or termination of the agreement. The Vendor agrees to notify the City if any of its employees or other representatives having access to the City's information security assets is terminated or otherwise ceases to provide services to the City. The Vendor agrees to advise all such employees and other representatives of the PCI DSS requirements under this agreement.

The Vendor acknowledges and agrees that any remote access granted to the City's information systems will be on a per use basis and will require prior authorization for defined purposes and periods. The Vendor agrees that if there is a change in the scope or timing of the access required, the Vendor will immediately inform the City by emailing Security@coquitlam.ca and calling 604-927-3600.

The Vendor agrees to report loss, theft, misuse or potential misuse of passwords, access cards, keys or other control credentials to the City within 24 hours by emailing facilitiescustomerservice@coquitlam.ca and security@coquitlam.ca, to take immediate steps to mitigate the harmful effects of such incident and to report the incident and all relevant details to the City by calling 604-927-3600 and emailing security@coquitlam.ca. The Vendor agrees to cooperate with and assist the City in the investigation and resolution of any such incident.

Coquitlam

City of Coquitlam
Terms and Conditions of Purchase
Payment Card Industry (PCI) Data Security Standard (DSS)

4. Breach Protocol

Upon discovering or otherwise becoming aware of the loss, theft, misuse or potential misuse of passwords, access cards, keys or other control credentials or an incident that may put the City's information at risk (a "Security Incident"), the Vendor will take all reasonable measures to mitigate the harmful effects of the Security Incident and to protect the City's systems and information from any further compromise, as well as any other actions that may be required by applicable law as a result of such Security Incident.

Without limiting the generality of the foregoing, the Vendor will immediately investigate any Security Incident and notify the City of such Security Incident no later than 24 hours following discovery or notice of such Security Incident. The Vendor's receipt of a reasonably credible threat by a credible third party, whether known or unknown, to cause a Security Incident will be investigated by the Vendor and evaluated in the same manner as if discovered by Vendor.

The Vendor's notification to the City of a Security Incident as required herein will consist of a telephone call to the City at 604-927-3600 (or such other telephone number as may be designated by the City from time to time) followed immediately by an e-mail to Security@coquitlam.ca. Such notification will include the following information (as applicable):

(a) the nature and extent of the City information potentially involved in the Security Incident;
(b) identification of the individuals whom the Vendor knows or reasonably believes to have improperly used, disclosed or accessed City information;
(c) description of where the Vendor knows or has reason to believe the affected City information has been improperly transmitted, sent or utilized;
(d) a description of the probable causes of the Security Incident;
(e) any other information determined necessary by mutual agreement of the parties for City to respond to the Security Incident; and
(f) complete Vendor incident response lead contact information.

If notification to affected individuals is required as a result of the Security Incident, the City may require the Vendor to provide such notification at its sole cost and expense, provided that the City will approve in advance the time, manner and content of any such notification.

The Vendor will provide a written report of its investigation to the City within ten (10) business days following its discovery of any Security Incident. Such report will include, but not be limited to, the information specified above and a full, detailed corrective action plan, including information on measures taken by the Vendor to halt or contain the Security Incident.