PCI DSS COMPLIANCE & CARDHOLDER DATA RISK MITIGATION EXHIBIT 1

It is hereby agreed that:

1) Vendor agrees that it and/or its subcontractors, as applicable, are responsible for the security of cardholder data that it/they possess, including the functions relating to storing, processing, and transmitting of the cardholder data.

2) Vendor affirms that, as of the effective date of this addendum, it and/or its subcontractors, as applicable, have complied with all applicable requirements to be considered PCI DSS compliant, and has/have performed the necessary steps to validate its/their compliance with the PCI DSS.

3) Vendor agrees to supply the current status of Vendor's PCI DSS compliance status and/or that of its subcontractors, as applicable, and evidence of its/their most recent validation of compliance upon execution of this addendum to the City. Vendor must supply to the City a new status report and evidence of compliance for Vendor and/or its subcontractors, as applicable, at least annually.

4) Vendor will immediately notify the City if it learns that it and/or any of its subcontractors, as applicable, is/are no longer PCI DSS compliant and will immediately provide the City with steps being taken to remediate the non-compliance status.

5) Vendor will give immediate notice to the City of any actual or suspected unauthorized disclosure of, access to, or other breach of cardholder data of the City's customers. Vendor and/or its subcontractors, as applicable, will cooperate with representatives or agents of the City and/or payment card industry in conducting a thorough security review of the operations, systems, records, procedures, rules, and practices of the Vendor and/or its subcontractors, as applicable.

6) To complement PCI DSS compliance activities, Vendor and/or its subcontractors, as applicable, will undergo an annual System and Organizational Control SOC-1/SOC-2 audit to assess the entity's controls over the security, availability, confidentiality, processing integrity, and privacy of users' data, and provide a copy/copies of the audit report(s) to the City upon request.

7) Vendor acknowledges that it will indemnify, defend, save and hold harmless the City, its officials, employees and authorized agents for any failure of the Vendor and/or its subcontractors, as applicable, to be and remain PCI DSS compliant and maintain the security of cardholder data that it/they possess.

8) Vendor agrees to provide current appropriate cybersecurity insurance coverage with the City as the named certificate holder for the duration of the agreement.

Note: This exhibit for use with applicable new agreements.