FIN 2.10 Technical analysis requirements

Bureaus using electronic commerce service applications that enable receipt of electronic check or payment card transactions such as Visa/MasterCard via the web will route the electronic receipts approval requests through the City's centralized Payment Processing Gateway (PPG) for approval or disapproval by the City's merchant services provider. PPG is a City-developed electronic payment processing web service and connection mechanism to route payment card receipts to the City's payment processing provider, with integration to support the reconciliation process. These requirements are described in further detail in the City's Technology Services Administrative Rules and other policies.

Payment Card Industry - Data Security Standard (PCI-DSS) compliance:
Payment card companies such as Visa, MasterCard and American Express created PCI-DSS, which represents a common set of industry tools and measurements to help ensure the safe handling of sensitive payment card information. PCI-DSS compliance requires adequate security controls when storing, processing and transmitting sensitive cardholder data. Sensitive cardholder data includes the personal account number (cardholder account number) and track information (data on the magnetic strip). Payment card companies, such as Visa and MasterCard, enforce the PCI-DSS standards, set merchant levels, set fees and penalties, and conduct management assessments.

The merchant services provider or vendor bank is the "acquirer" and the liaison between the City and the payment card associations. The associations and vendor bank determine the City's PCI merchant level based on volume and scope of processing activity. For purposes of determining merchant levels and the extent of a breach, payment card programs can be regarded as independent if it can be demonstrated that they are segregated (i.e., they are not on a common server or use the same gateway, etc.).

PCI-DSS primarily addresses breach of electronic data and electronic data processing. However, voice recordings of payment card data, printed receipts and paper reports of sensitive cardholder data are also within the scope of PCI-DSS.

If it is determined that a security breach has occurred and cardholder data has been compromised, the association may assess fees and/or fines against the vendor bank and ultimately the City. All merchants, including the City, are responsible for self-compliance as well as ensuring the compliance of third-party service providers or agents acting on behalf of the City. A service provider may be any agent to which the City provides cardholder data or provides access to cardholder data. Services providers must be validated and registered with the PCI Security Standards Council.