EXHIBIT A

CFMP 2.17 Payment Card Industry Compliance
Binding City Policy
BCP-FIN 2.17

Scope
The purpose of this policy is to establish minimum compliance standards for the acceptance and processing of payment card transactions for the City of Portland.

Policy
The ability to provide payment card options to customers is critical to the City's business goals. The City is committed to protecting customer payment card information.

It is the City's policy that all bureaus, offices, and designated agents of the City of Portland be fully compliant with the Payment Card Industry Data Security Standard (PCI DSS) established and maintained by the PCI Security Standards Council.

Compliance requires, but is not limited to, meeting the following criteria:

1. *Services* – Payment services must be processed in accordance with the PCI DSS.
2. *Devices* – Payment devices must meet PCI PIN Transaction Security (PTS) validation and utilize point-to-point encryption technology.
3. *Software* – Payment software must be compliant with the PCI Payment Application Data Security Standard (PA DSS).

Compliance with this policy also requires bureaus to take all appropriate steps, as outlined later in this policy, to ensure the compliance of designated agents.

Definitions
"Attestation of Compliance (AOC)" means the signed document evidencing compliance with PCI DSS.

"Payment Card" means a credit or debit card with a branded logo (Visa, MasterCard, Discover, or American Express) on the face of the card and which is used to pay for goods and services.

"Payment Card Industry (PCI)" means the council originally formed in 2006 by American Express, Discover, JCB International, MasterCard, and Visa Inc., with the goal of managing the ongoing evolution of the PCI DSS.

"Payment Card Industry Data Security Standard (PCI DSS)" means a set of requirements, as amended, that address the handling, transmission, and storage of sensitive cardholder data. Current standards are maintained at:
https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security

"Payment Application Data Security Standard (PA DSS)" means a set of requirements that address software applications that store, process, or transmit cardholder data where the payment application is sold, distributed, or licensed to third parties.

Bureau Responsibility for Payment Card Processing Services
City bureaus may choose to accept Payment Cards in person, by phone or online. City bureaus that choose to accept Payment Cards shall comply with all applicable City policies including but not limited to FIN-2.10 - Electronic Payment Processing Services, BTS-2.17 - Payment Card Security Standards, BTS-3.01 - E-Government Services and HRAR-4.08 - Information Technologies.

Bureau Development and Management of Contracts for Third-Party Vendors
Bureaus may choose to contract with a third-party vendor as a designated agent to provide Payment Card processing services. If contracting for such services, bureaus are required to work with the Technology Group in Procurement Services to ensure the contract includes clauses which require substantial indemnification for security or data breaches, special insurance provisions, annual provision of an Attestation of Compliance (AOC) by the vendor, penalties for an inability to deliver an AOC, and termination for non-compliance.

Bureaus are required to discuss with the Treasury Division of the Bureau of Revenue and Financial Services (Treasury Division) and the Bureau of Technology Services (BTS) any proposed use of Payment Card services during the development of a Request for Proposal (RFP) and during contract review for such services. Approval by the Treasury Division and BTS is required before a bureau can proceed with the RFP and before the final contract negotiated by Procurement Services can be approved by the bureau and, if necessary, City Council.

Bureaus are responsible for sending AOC's for their designated agents to Treasury and to BTS-Information Security.

In the event a designated agent is in breach of contract for failure to deliver an AOC, bureaus are required to work with the Treasury Division and BTS to implement remediation plans, up to and including termination of the vendor relationship and replacement with a PCI-compliant system or implementation of an alternate PCI-compliant workaround.

Designated Agents' Responsibility
All designated agents, such as third-party Payment Card processors acting on behalf of a City bureau, shall maintain a current AOC for the period of time during which they are doing business with the City of Portland. Designated agents that are not able to provide current AOC's will be in material breach of their contract with the City and subject to penalty and termination.

Policy Responsibility
The Treasury Division of the Bureau of Revenue and Financial Services, and the Bureau of Technology Services are responsible for developing and implementing this policy and providing technical assistance to the bureaus. The Treasury Division and BTS shall review this policy at least annually and update it as needed to reflect changes to business objectives or the risk environment.

Related Policies
FIN 2.10 Electronic Payment Processing Services
BTS 2.17 Payment Card Security Standards
BTS 3.01 E-Government Services
HRAR 4.08 Information Technologies

History
Adopted by City Council DATE