Credit and Debit Card Processing

Purpose

The District accepts credit cards and debit cards for payment of goods and services, including but not limited to tickets for athletic, theatrical, and musical events, under controlled conditions to protect against the exposure and possible theft of account and personal cardholder information that has been provided to the District; and to comply with Payment Card Industry Data Security Standards ("PCI DSS") requirements. The District adheres to these PCI DSS requirements to help limit its liability and continue to process payments using payment cards.

Scope

This policy applies to all District departments, employees, contractors, consultants, temporary employees, and other workers ("District Personnel"). This policy is applicable to any area that processes, transmits, or handles cardholder information in a physical or electronic format. All computers and electronic devices at the District involved in processing payment card data are governed by the PCI DSS requirements. This includes servers which store payment card numbers, workstations which are used to enter payment card information into a central system (for example, ordering tickets over the phone or activity fee payments), and any computers or credit/debit card swipe devices through which the payment card information is transmitted.

Policy

All transactions that involve the transfer of credit card, debit card, or mobile wallet information must be performed on systems approved by the Business Office and Technology Department. The District shall comply with relevant PCI DSS requirements and work with any third-party vendors of payment processing to ensure their PCI DSS compliance. The District shall also make reasonable efforts to comply with any third-party vendor recommended policies and best practices as provided by the vendor.

Security Measures

- District Personnel engaged in the transmission, processing, or access of credit/debit card, mobile wallet, or electronic payments shall receive training on the entirety of this policy and relevant PCI DSS requirements.
- In no case shall a Primary Account Number (the 16-digit number printed on the front of a credit/debit card), the expiration date of a credit/debit card, or the three-digit security code printed on the back of a credit/debit card be transmitted or distributed via unencrypted channels such as e-mail, text messages, instant messaging, or other similar communication methods.
- In no case shall credit card, debit card, or mobile wallet information be stored in or on District owned computers, electronic devices, databases, or systems unless needed for a legitimate business purpose. Such information shall be isolated and stored securely, with access available only to authorized personnel with a legitimate need for such information as determined by the Business Office. After there ceases to be a legitimate business purpose for storing such information, it shall be promptly and securely deleted and/or destroyed.
- On any system where payment information such as account numbers or credit/debit card information is transmitted, processed, or accessed, the District shall install Anti-Virus software and set it to update automatically. The Anti-Virus software shall log data for at least one full calendar year.
- Systems and devices used to facilitate the transmission, processing, or access information such as account numbers or credit/debit card information shall be regularly updated or patched when such updates are available. Critical security patches shall be installed within thirty (30) days of their release.
- Systems and devices used to facilitate the transmission, processing, or access information such as account numbers or credit/debit card information shall have a PCI DSS compliant firewall system in place to prevent unauthorized traffic.
- Physical documents or hard copies containing account information or credit/debit card information shall be destroyed immediately after it is no longer needed. Any such materials that are not immediately destroyed (for example, placed in a "to-be-shredded" container) shall be secured and accessible only by authorized personnel.
- The Business Office and Technology Department shall review the procedures implemented pursuant to this policy to test the efficacy of security systems and make adjustments as needed.

Specific Security Measures for Point of Sale ("POS") Devices

A Point of Sale ("POS") device is any hardware, software, or piece of equipment that enables the District or District Personnel to process credit card, debit card, or mobile wallet payments.

- District Personnel using POS devices shall receive training on the entirety of this policy and relevant PCI DSS security measures for processing electronic, credit/debit card, and mobile wallet transactions.
- Before each use, POS devices shall be visually inspected by District Personnel for evidence of any tampering, modification, or damage to the device. If such evidence is found, the POS device shall not be used to process transactions and a report shall immediately be made to the Business Office and Technology Department.
- Third parties shall not be permitted to handle the POS device, including persons claiming to need to perform maintenance on the POS device or replace the POS device. All maintenance and replacement of POS devices will be performed by or at the direction of the Technology Department.
- If a POS device is required to be connected to any District owned computer, terminal, device, or equipment in order to function, the District shall ensure that those computers, terminals, devices, or pieces or equipment are only connected to secure, encrypted networks.
- Only authorized District Personnel will be permitted to handle POS devices. District Personnel should immediately report the handling or use of POS devices by unauthorized persons.

Adopted: 9/26/2022
Reviewed:
Revised: