Metropolitan Government of Nashville and Davidson County - Finance Dept. Policy: Payment Card Industry Compliance

Effective Date: August 2006
Revision Date: September 16, 2025
Policy Number: 3.7
Sponsor: Office of the Treasurer

Purpose

Metropolitan Government of Nashville and Davidson County (Metro) is committed to complying with the Payment Card Industry Data Security Standards (PCI DSS). This policy will establish uniform guidelines governing the acceptance of credit and debit cards as a form of payment by departments and agencies of Metro and provide procedures to help prevent loss or disclosure of customer information, including credit card numbers. PCI DSS requirements apply to all transactions surrounding the payment card industry and the merchants of organizations that accept these cards as forms of payment. Metro must show evidence of and maintain compliance with PCI DSS in the Departments that accept credit card payments.

Definitions

Breach: A suspected or confirmed event where there has been unauthorized access, loss, or theft (to a system, network, material, or records) to Cardholder Data. This includes systems, networks, or physical locations where Cardholder Data is collected, processed, stored, or transmitted.

Cardholder Data: The elements of payment card information that are required to be protected. These elements include Primary Account Number, Cardholder Name, Expiration Date and the Service Code.

Cardholder Data Environment (CDE): The people, processes, and technologies that store, process, or transmit data, including cardholder or sensitive authentication data. Technology components include network devices, servers, computing devices, and applications.

Payment Card Industry Data Security Standards (PCI DSS): The security requirements defined by the Payment Card Industry Security Standards Council and the five major Payment card Brands: Visa, MasterCard, American Express, Discover, JCB to provide specific guidelines for safeguarding cardholder information.

PCI Compliance Security Assessor: A position in the Treasurer’s Office working to enhance the quality, reliability, and consistency of the organization’s internal PCI DSS self-assessments, and support the consistent and proper application of Data Security Standards and controls.

Sensitive Authentication Data: The elements of payment card information that are also required to be protected but never stored. These include Magnetic Stripe (i.e., Track) data, CAV2, CVC2, CID, or CVV2 data and PINs/PIN Block.

General Policies

To accept credit and debit card payments, each Metro Department must work with the Treasurer’s Office and comply with this policy and the PCI Compliance Procedures.

The Treasurer’s Office will contract with a third-party processor to handle Metro’s credit and debit card transactions which will be funded through a service fee model charged by the processor to the cardholder as required by state law. In compliance with state law, any Metro department wishing to waive the service fee and directly pay the interchange fees associated with credit and debit card transactions must obtain approval to do so from Metro Council or appropriate governing body.

All departments integrating credit and debit card receipts into a cashiering system or software must utilize Metro's contracted gateway and processor except in cases defined in 1.4.

Departments with unique business operations or specific requirements not provided by the contracted Merchant Services provider may submit request to the PCI Compliance Security Assessor in the Treasurer's Office in accordance with the Payment Processor Exception Process.

Departments accepting credit and debit card payments must provide the Treasurer's Office with a Department Responsible Persons (DRP) (Primary and Alternate) who will be responsible for reviewing and acting upon any inquiry, dispute or chargeback as communicated by the gateway or processor for a specific Merchant ID (MID).

The DRP will also serve as the point of contact for PCI-DSS compliance responsibilities within the department.

Daily settlement of all credit and debit card transactions is handled directly by the gateway or processor in an automated batch process. Each Metro Department accepting credit and debit cards is responsible for recording receipts into the general ledger within two (2) business days of bank settlement in accordance with Metro's Cash Receipts procedures produced and maintained by Division of Accounts.

The PCI Compliance Security Assessor must approve payment applications and card processing devices before being connected to the Metro network.

Departments are responsible for communicating to customers any Service Fees charged when paying with a credit or debit card.

<u>Prohibited Actions</u>

Metro Departments shall not store unmasked Cardholder Data or Sensitive Authentication Data, including magnetic stripe or track data and CAV2, CVC2, CID, or CVV2, in hardcopy or electronic form.

Metro Departments shall not accept credit and debit card payments via fax, e-mail, text, or voicemail.
Calls in which debit and credit card payments are taken must never be recorded, whether the calls are directly to a Metro employee or to an IVR system.

Metro Departments accepting credit/debit card payments via mail must shred the cardholder data once the payment has been processed. The Primary Account Number (PAN) must be immediately and completely redacted from the remittance authorization in accordance with PCI-DSS.

Metro Departments shall not leave any credit/debit card information out on desktops or anywhere else where others may have access to it.

Metro Departments shall not disclose or release any credit and debit card information for any purpose other than payment processing.

<u>Responsibilities</u>

All employees involved with the transmission, storage, or processing of Cardholder Data (including systems that can impact the security of payment card data) must review and acknowledge this policy and associated PCI Compliance procedures.

All employees with access to the Metro Cardholder Data Environment (CDE), must complete training in accordance with PCI-DSS. Required training will be conducted upon hire and annually.

Metro Departments accepting credit and debit card payments are responsible for ensuring that all credit and debit card data is handled in a secure manner and that all staff have completed the required training.

Metro Directors and Agency Heads are responsible for ensuring that the department/agency is PCI-DSS Compliant.
Metro Directors and Agency Heads are responsible for ensuring that all staff exposed to cardholder data have

reviewed and understand all applicable policies and procedures involving credit/debit card payments and processing.

Departments accepting credit and debit card payments must report any suspicious or suspected Breach of cardholder information immediately to the Treasurer, the Metro Chief Information Security Officer (CISO) and Internal Audit.

Metro Departments are required to follow all relevant laws, regulations, rules and policies applicable to credit and debit card acceptance. Specifically, adherence to the following is mandatory:

- Payment Card Industry Data Security Standard
- Visa, MasterCard, Discover and American Express credit Card processing rules and regulations
- This policy and all related Metro cash management policies
- Any contracted agreements with integrated credit card gateway and processer provider(s)

Resources and Attachments

PCI Security Standards Council Web site: https://pcisecuritystandards.org/

For questions or concerns not addressed in this policy, please email PCICompliance@nashville.gov

Payment Card Procedures

Payment Processor Exception Process

Applicable Local, State or Federal Regulations

Metro. Charter art. 8 ,§ 8.103: The director of finance shall be responsible to the mayor for the administration of the financial affairs of the metropolitan government.

Metro. Charter art. 8, § 8.104: The budget officer, with the advice and assistance of the chief accountant, shall write, revise and maintain a proper standard procedure instruction manual to be followed by all officers, departments, boards and other agencies of the government to ensure uniform accounting and budgetary procedures.

Metro. Charter art. 8, § 8.105: The chief accountant shall maintain a general accounting system and such cost accounting records as shall be required by the director of finance.

Metro. Charter art. 8, § 8.106: The metropolitan treasurer shall supervise and be responsible for the custody and disbursement of all funds belonging to the metropolitan government and all funds handled by metropolitan government officers as agents or trustees except as otherwise provided in this Charter or by ordinance or general law not inconsistent with this Charter.

Metro. Code art. 8, ch. 1, § 8.106

Tenn. Code Ann. § 9-1-108 (as amended by Pub. Acts 2001, ch. 348)

Metro. Ord. No. BL2001-777

Metro. Ord. No. BL2006-1093

Metro. Ord. No. BL2006-1266

Metro. Ord. No. BL2008-218

Associated Policies

None.

Effective Date

This Policy Statement shall become effective upon issuance and shall be applied to all Metro departments and agencies.

Approvals

Approval of the Director of Finance

I hereby approve this Policy Statement of the Department of Finance and as such agree with and authorize the actions necessary to implement its requirements.

Jenneen Reed

Director of Finance

Date: September 16, 2025