Payment Card Industry Data Security Standards

Policy

MAWA leases a debit/credit card machine terminal to receive payments for memberships, workshop fees, fundraisers, donations, etc. Payments may be made in person by tap or keyed entry or by manual entry by MAWA employees over the phone.

Credit Card Information is made up of 4 elements:

1. Primary Account Number (PAN), which is the number embossed on the face of the card
2. Cardholder Name, which appears on the face of the card
3. Service Code, which is a three-digit code encoded on the magnetic strip
4. Expiration Date

Security Codes are the CVV/CVC value found on the reverse side of most cards.

Credit Card Information and Security Codes

Under no circumstances are security codes (CVV/CVC) recorded or stored in any way. MAWA employees may enter this information directly into a terminal from a card or cardholder verbally. It is erased after authorization.

There are no electronic records kept on computers, laptops or workstations that include credit card information (primary account number, expiration date, card holder name and service code).

Credit card primary account numbers that have been manually written down are kept in a secure file. Documents containing PAN data will be shredded after being entered into a terminal or no longer needed. Records are destroyed within two years.

Only approved employees shall handle PAN data. No credit card information will be shared with unauthorized personnel. Any employee found to have violated this policy will be subject to disciplinary action.

Credit Card Processing

The Credit Card processing terminal is only used for approved sales and donations.

Employees may ask to see identification for purchases over $500.

Equipment

MAWA's leased equipment that stores, processes and transmits PAN data complies with Payment Card Industry Data Security Standards (PCI DSS).

The Executive Director oversees the lease agreement and any changes in equipment. The Executive Director and Administrative Coordinator have the authorization code for the terminal and are the contacts for the merchant service provider. Authorization codes and passwords for the terminal are kept confidential.

Only verified individuals can inspect, repair or change equipment. Information about the terminal and serial numbers are kept on file. If tampering is suspected transactions will not be processed through the terminal. The merchant service provider will be contacted and the device will be secured to prevent further tampering. The Executive Director will follow incident response and reporting protocols.

Incident Response

The Executive Director is notified if there is unauthorized access to the network; theft, loss or a compromise of credit card information; loss of credit card terminal; destruction of facilities; or loss of paper records containing credit card information. The Executive Director will notify the merchant bank within 24 hours and will follow the instructions set out by the merchant bank.

Training

The Executive Director and Administrative Coordinator oversee training of other staff including the process of gathering and submitting receipts. Other contract workers can be authorized to use the terminal by the Executive Director.

Authorized staff must read all policies and must be made aware of any changes. Employees are asked to review the *Security Awareness: Guide to Credit Card Acceptance* Booklet.

Network Security

Scanning and penetration testing by a qualified vendor working with the merchant bank are performed quarterly. Failed vulnerability scans must be resolved.

The process to identify threats and vulnerabilities, perform risk assessment and secure information is reviewed annually. All policies are reviewed annually and updated as required to satisfy current requirements.

This policy was developed with reference to CSRSI (Centre for Scientific Research and Statistical Information) and PCI DSS (Payment Card Industry Data Security Standards).