POLICY/PURPOSE

Mid-Michigan District Health Department (MMDHD) accepts credit/debit card payments for services. It is the policy of the agency to ensure that information is handled and disposed of in a manner that protects customer information, complies with applicable law and meets the obligation to comply with the data security standards required by the Payment Card Industry (PCI).

The set of standards referred to as the Payment Card Industry’s Data Security Standards (PCI-DSS) sets forth security standards for any organization that accepts, captures, stores, transmits and/or processes credit/debit card information either manually or through an automated system.

Merchant credit/debit card transactions are monetary transactions and are subject to the same control and reconciliation process as cash transactions. Failure to comply with PCI-DSS may result in the loss of the ability to process credit/debit cards and substantial fines if a breach occurs.

The components of PCI-DSS apply to all forms of transaction which includes items such as maintaining a secure network, protection of data, encrypted transmissions of data, and maintenance of a vulnerability management program which includes the use of anti-virus software. PCI-DSS also requires that the agency complete an annual self-assessment questionnaire. The agency must comply with all information required per the self-assessment.

Employees are responsible for protecting credit/debit card information. Physical documents that contain any credit/debit card information must be stored in secured access-controlled locations. The validation code and personal identification number should not be stored in any form. In no case, should credit card information be transmitted via insecure protocols such as email or text message.

Any suspected theft of information or inappropriate activity must be reported immediately to the Administrative Services Division Director.