Information Security Policy

Cheboygan Area Arts Council

Revision 3 – December 2, 2025

Please see PCI DSS v4.x Quick Reference Guide for an overview of the security requirements this policy implements.

Part 1 - Account Data Protection

Processes and mechanisms for protecting stored account data, fulfilling PCI DSS 4.x Requirement 3 are defined and understood.

All security policies and operational procedures that are identified in requirement 3 are:

- Documented.
- Kept up to date.
- In use.
- Known to all affected parties.

Sensitive authentication data (SAD) is not stored after authorization

SAD is not stored after authorization, even if encrypted. All sensitive authentication data received is rendered unrecoverable upon completion of the authorization process.

The full contents of any track (magnetic stripe data or equivalent on a chip) are not stored upon completion of the authorization process.

The card verification code is not stored upon completion of the authorization process.

The personal identification number (PIN) and the PIN block are not stored upon completion of the authorization process.

Access to displays of full PAN and ability to copy PAN are restricted.

PAN is masked when displayed (the BIN and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than the BIN and last four digits of the PAN.

Part 2 - Access Control Measures

Access to system components and data is appropriately defined and assigned, fulfilling requirement PCI DSS 4.x Requirement 7.

Access is assigned to users, including privileged users, based on:

- Job classification and function.
- Least privileges necessary to perform job responsibilities.

Physical access to cardholder data is restricted as per PCI DSS 4.x Requirement 9.

Media with cardholder data is securely stored, accessed, distributed, and destroyed.

All media with cardholder data is physically secured.

Offline media backups of cardholder data are are not created or stored.

No media with cardholder data is sent outside the facility or distributed.

Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution.

POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following:

- Maintaining a list of POI devices.
- Periodically inspecting POI devices to look for tampering or unauthorized substitution.
- Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices.

An up-to-date list of POI devices is maintained, including:

- Make and model of the device.
- Location of device.
- Device serial number or other methods of unique identification.

POI device surfaces are periodically inspected to detect tampering and unauthorized substitution.Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes:

- Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices.
- Procedures to ensure devices are not installed, replaced, or returned without verification.
- Being aware of suspicious behavior around devices.
- Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel.

Part 3 – Security Information Policy

A comprehensive information security policy (this document) that governs and provides direction for protection of the entity's information assets is known and current, and fulfills PCI DSS 4.x requirement 12.

An overall information security policy is:

- Established.
- Published.
- Maintained.
- Disseminated to all relevant personnel, as well as to relevant vendors and business partners.

The information security policy is:

- Reviewed at least once every 12 months.
- Updated as needed to reflect changes to business objectives or risks to the environment

The security policy clearly defines information security roles and responsibilities for all personnel, and all personnel are aware of and acknowledge their information security responsibilities.

Security awareness education is an ongoing activity.

A formal security awareness program is implemented to make all personnel aware of the entity's information security policy and procedures, and their role in protecting the cardholder data.

Risk to information assets associated with third-party service provider (TPSP) relationships is managed

A list of all third-party service providers (TPSPs) with which account data is shared or that could affect the security of account data is maintained, including a description for each of the services provided.

Written agreements with TPSPs are maintained as follows:

- Written agreements are maintained with all TPSPs with which account data is shared or that could affect the security of the CDE.
- Written agreements include acknowledgments from TPSPs that TPSPs are responsible for the security of account data the TPSPs possess or otherwise store, process, or transmit on behalf of the entity, or to the extent that TPSPs could impact the security of the entity's cardholder data and/or sensitive authentication data..

An established process is implemented for engaging TPSPs, including proper due diligence prior to engagement.

A program is implemented to monitor TPSPs' PCI DSS compliance status at least once every 12 months.

Information is maintained about which PCI DSS requirements are managed by each TPSP, which are managed by the entity, and any that are shared between the TPSP and the entity.

Suspected and confirmed security incidents that could impact the CDE are responded to immediately.

An incident response plan exists and is ready to be activated in the event of a suspected or confirmed security incident