REQUIREMENT #3: PROTECT STORED CARDHOLDER DATA

Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person.

PCI DSS CONTROL 3.1

Control Objective: The organization implements a process for to minimize the storage of cardholder data.

Standard: Data owners are required to determine the business requirements for data retention and securely dispose of cardholder data once the data is no longer necessary. This includes, but is not limited to: [37]

(a) Implement a data retention and disposal policy that covers cardholder data;
(b) Limiting cardholder data retention time to that which is required for legal, regulatory, and business requirements;
(c) Conducting a quarterly process (automatic or manual) to identify and securely delete stored cardholder data that exceeds defined retention requirements.
(d) Performing secure deletion of electronic-based cardholder data; and
(e) Shredding physical-based cardholder data.

Supplemental Guidance: Specific requirements for the retention of cardholder data are driven by business needs (e.g., cardholder data needs to be held for X period for Y business reasons) and documentation should exist to justify the business need.

Procedures: The City does not store cardholder data, and it is prohibited by any department to store cardholder data as the Primary Account Number (PAN), security codes, or information on the magnetic strip (track 1 or 2) electronically or physically. It is prohibited to transmit cardholder data through any end-user messaging technologies include, but are not limited to: facsimile (fax) machines, Electronic mail (e-mail), electronic forms, Instant messaging (IM),Chat, and Short Message Service (SMS). Storing or transmitting cardholder data via paper forms is also prohibited.

PCI DSS CONTROL 3.2

Control Objective: The organization does not store sensitive authentication data after authorization.

Standard: Asset custodians are required to ensure sensitive authentication data is not stored after authorization, even if it is encrypted. City of Waukesha is prohibited from storing: [38]

(a) The full contents of any track: [39]
    1. Tracks are from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere.
    2. This data is alternatively called the full track, track, track 1, track 2, and magnetic-stripe data.
(b) Storing the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions; [40] and
(c) Storing the Personal Identification Number (PIN) or the encrypted PIN block. [41]

Supplemental Guidance: The following data sources should be examined to verify that the full contents of any track from the magnetic stripe on the back of the card or equivalent data on a chip are not stored under any circumstance:

- Incoming transaction data;
- All logs (e.g., transaction, history, debugging, error);
- History files;
- Trace files;
- Several database schemas; and
- Database contents.

[37] PCI DSS v3.2 Requirement 3.1
[38] PCI DSS v3.2 Requirement 3.2
[39] PCI DSS v3.2 Requirement 3.2.1
[40] PCI DSS v3.2 Requirement 3.2.2
[41] PCI DSS v3.2 Requirement 3.2.3

Procedures: The City does not store cardholder data, and it is prohibited by any department to store cardholder data as the Primary Account Number (PAN), security codes, or information on the magnetic strip (track 1 or 2) electronically or physically. It is prohibited to transmit cardholder data through any end-user messaging technologies include, but are not limited to: facsimile (fax) machines, Electronic mail (e-mail), electronic forms, Instant messaging (IM),Chat, and Short Message Service (SMS). Storing or transmitting cardholder data via paper forms is also prohibited.

PCI DSS CONTROL 3.3

Control Objective: The organization masks the Primary Account Number (PAN) when displayed.

Standard: Data owners, in conjunction with asset custodians, are required to ensure the PAN is masked so no more than the first six (6) and last four (4) digits are the maximum number of digits allowed to be displayed and/or printed.[42]

Supplemental Guidance: Only users with a legitimate business need to see the full PAN are allowed an exception to this requirement.

Procedures: This is a functionality of the software that is used for collecting payments.

PCI DSS CONTROL 3.4

Control Objective: The organization implements a process to ensure Primary Account Numbers (PANs) are rendered unreadable anywhere PANs are stored.

Standard: Asset custodians, in conjunction with data owners, are required to implement technical measures to ensure PANs are not accessible by unauthorized users or processes by using any of the following approaches: [43]

(a) Render PANs unreadable anywhere PANs are stored, including on portable digital media, backup media, and in logs through the means of:
    1. One-way hashes based on strong cryptography (hash must be of the entire PAN);
    2. Truncation (hashing cannot be used to replace the truncated segment of PAN);
    3. Index tokens and pads (pads must be securely stored); or
    4. Strong cryptography with associated key-management processes and procedures; and

(b) Preventing decryption keys from being tied to user accounts, if disk encryption is used, rather than file- or column-level database encryption: [44]
    1. Logical access must be managed independently of native operating system access control mechanisms (e.g., by not using local user account databases).
    2. Decryption keys must not be tied to operating system-level user accounts.

Supplemental Guidance: Since it is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN, where hashed and truncated versions of the same PAN are present City of Waukesha's environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.

Procedures: The City does not store cardholder data, and it is prohibited by any department to store cardholder data as the Primary Account Number (PAN), security codes, or information on the magnetic strip (track 1 or 2) electronically or physically. It is prohibited to transmit cardholder data through any end-user messaging technologies include, but are not limited to: facsimile (fax) machines, Electronic mail (e-mail), electronic forms, Instant messaging (IM),Chat, and Short Message Service (SMS). Storing or transmitting cardholder data via paper forms is also prohibited.

PCI DSS CONTROL 3.5

Control Objective: The organization implements a key management strategy to protect keys used to secure cardholder data against disclosure and misuse.

Standard: Data owners are required to implement administrative and technical measures to protect keys used to secure cardholder data against disclosure and misuse, including the following: [45]

(a) Maintain a documented description of the cryptographic architecture that includes: [46]
    1. Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date;
    2. Description of the key usage for each key; and
    3. Inventory of any Hardware Security Modules (HSMs) and other Secure Cryptographic Devices (SCDs) used for key management;

[42] PCI DSS v3.2 Requirement 3.3
[43] PCI DSS v3.2 Requirement 3.4
[44] PCI DSS v3.2 Requirement 3.4.1
[45] PCI DSS v3.2 Requirement 3.5
[46] PCI DSS v3.2 Requirement 3.5.1

(b) Cryptographic key access shall be restricted to the fewest number of custodians necessary; [47]
(c) Cryptographic key access shall be securely stored at all times using one of the following methods: [48]
    1. Encrypted with a key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data encrypting key;
    2. Within a secure cryptographic device (such as a host security module (HSM) or PTS-approved point-of-interaction device); or
    3. As at least two full-length key components or key shares, in accordance with an industry-accepted method; and
(d) Cryptographic keys must be securely stored in the fewest possible locations and forms. [49]

Supplemental Guidance: This requirement also applies to key-encrypting keys used to protect data-encrypting keys. This requires that key-encrypting keys must be at least as strong as the data-encrypting key.

Procedures: The City does not store cardholder data, and it is prohibited by any department to store cardholder data as the Primary Account Number (PAN), security codes, or information on the magnetic strip (track 1 or 2) electronically or physically. It is prohibited to transmit cardholder data through any end-user messaging technologies include, but are not limited to: facsimile (fax) machines, Electronic mail (e-mail), electronic forms, Instant messaging (IM),Chat, and Short Message Service (SMS). Storing or transmitting cardholder data via paper forms is also prohibited.

PCI DSS CONTROL 3.6

Control Objective: The organization documents and implements key management processes and procedures for cryptographic keys used for encryption of cardholder data.

Standard: Data owners are required to document and implement key management processes and procedures for cryptographic keys used for encryption of cardholder data that includes the following: [50]
(a) Procedures for the generation, distribution, and storage of keys:
    1. Generation of strong cryptographic keys; [51]
    2. Prevention of unauthorized substitution of cryptographic keys; [52]
    3. Distribution of cryptographic keys using secure methods; [53] and
    4. Secure storage of cryptographic keys; [54]
(b) Changing cryptographic keys that have reached the end of their ~~cryptoperiod~~crypto period: [55]
    1. After a defined period of time has passed and/or after a certain amount of ciphertext has been produced by a given key;
    2. As defined by the associated application vendor or key owner; or
    3. Based on industry-recognized leading practices and guidelines (e.g., NIST Special Publication 800-57).
(c) Retiring or replacing keys when the integrity of the key has been weakened or the keys are suspected of being compromised: [56]
    1. Retiring or replacing may be performed by archiving, destruction, and/or revocation of keys.
    2. Keys should be considered compromised by the departure of an employee with knowledge of a clear-text key.
(d) Split knowledge and dual control, if manual, clear-text cryptographic key management operations are used. If applicable, these operations require procedures that require two or three people, each knowing only their own key component, to reconstruct the whole key; [57] and
(e) Requiring cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities. [58]

[47] PCI DSS v3.2 Requirement 3.5.2
[48] PCI DSS v3.2 Requirement 3.5.3
[49] PCI DSS v3.2 Requirement 3.5.4
[50] PCI DSS v3.2 Requirement 3.6
[51] PCI DSS v3.2 Requirement 3.6.1
[52] PCI DSS v3.2 Requirement 3.6.7
[53] PCI DSS v3.2 Requirement 3.6.2
[54] PCI DSS v3.2 Requirement 3.6.3
[55] PCI DSS v3.2 Requirement 3.6.4
[56] PCI DSS v3.2 Requirement 3.6.5
[57] PCI DSS v3.2 Requirement 3.6.6
[58] PCI DSS v3.2 Requirement 3.6.8

Supplemental Guidance: Numerous industry standards for key management are available from various resources including NIST, which can be found at http://csrc.nist.gov.

Procedures: The City does not store cardholder data, and it is prohibited by any department to store cardholder data as the Primary Account Number (PAN), security codes, or information on the magnetic strip (track 1 or 2) electronically or physically. It is prohibited to transmit cardholder data through any end-user messaging technologies include, but are not limited to: facsimile (fax) machines, Electronic mail (e-mail), electronic forms, Instant messaging (IM),Chat, and Short Message Service (SMS). Storing or transmitting cardholder data via paper forms is also prohibited.

PCI DSS Control 3.7

Control Objective: The organization ensures that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.

Standard: Asset custodians and data owners are required to ensure that the PCI DSS Cybersecurity Policy and appropriate standards and procedures for protecting stored cardholder data are kept current and disseminated to all pertinent parties. [59]

Supplemental Guidance: Personnel need to be aware of and following security policies and documented operational procedures for managing the secure storage of cardholder data on a continuous basis.

Procedures: The City does not store cardholder data, and it is prohibited by any department to store cardholder data as the Primary Account Number (PAN), security codes, or information on the magnetic strip (track 1 or 2) electronically or physically. It is prohibited to transmit cardholder data through any end-user messaging technologies include, but are not limited to: facsimile (fax) machines, Electronic mail (e-mail), electronic forms, Instant messaging (IM),Chat, and Short Message Service (SMS). Storing or transmitting cardholder data via paper forms is also prohibited. ~~[insert a description of the actual procedures that you follow to meet this requirement]~~

Requirement #4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.

PCI DSS Control 4.1

Control Objective: The organization uses strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks.

Standard: To safeguard sensitive cardholder data during transmission, asset custodians are required to ensure the following: [60]

(a) Only trusted keys and certificates are accepted;
(b) Strong cryptography and security protocols are used to safeguard sensitive cardholder data during transmission over open, public networks. Examples of technologies that support this requirement include, but are not limited to:
    1. Trans Layer Security (TLS) v1.2 or higher;
    2. IP Security (IPSEC);
    3. Secure Shell (SSH) v2 or higher; and
    4. Secure File Transfer Protocol (SFTP) / File Transfer Protocol - Secure (FTP-S); and
(c) Wireless networks transmitting cardholder data or connected to the Cardholder Data Environment (CDE), use industry-recognized leading practices (e.g., IEEE 802.11i) to implement strong encryption for authentication and transmission. [61]

Supplemental Guidance: Examples of open, public networks that are in scope of the PCI DSS include but are not limited to:

- The Internet;
- Wireless technologies;
- Global System for Mobile communications (GSM); and

[59] PCI DSS v3.2 Requirement 3.7
[60] PCI DSS v3.2 Requirement 4.1
[61] PCI DSS v3.2 Requirement 4.1.1

- General Packet Radio Service (GPRS).

Procedures: ~~[insert a description of the actual procedures that you follow to meet this requirement]~~The encryption to the payment gateway from the card readers is handled by the payment processor.

PCI DSS CONTROL 4.2

Control Objective: The organization prohibits the transmission of unprotected Primary Account Numbers (PANs) by end-user messaging technologies.

Standard: City of Waukesha prohibits the transmissions of unprotected PANs by end-user messaging technologies. [62]

Supplemental Guidance: Examples of end-user messaging technologies include, but are not limited to:

- Electronic mail (e-mail);
- Instant messaging (IM);
- Chat; and
- Short Message Service (SMS)

Procedures: The City uses PCI DSS data loss prevention polices across the Office 365 tenant. This includes SharePoint,OneDrive, Teams, and Email. ~~[insert a description of the actual procedures that you follow to meet this requirement]~~

PCI DSS CONTROL 4.3

Control Objective: The organization ensures that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.

Standard: Asset custodians and data owners are required to ensure that the PCI DSS Cybersecurity Policy and appropriate standards and procedures for encrypting transmissions of cardholder data are kept current and disseminated to all pertinent parties.[63]

Supplemental Guidance: Personnel need to be aware of and following security policies and operational procedures for managing the secure transmission of cardholder data on a continuous basis.

Procedures: ~~[insert a description of the actual procedures that you follow to meet this requirement]~~IT Security Policies are posted on the City's intranet page, are emailed to staff, and we also do security awareness training with staff that handle credit card payments.

[62] PCI DSS v3.2 Requirement 4.2
[63] PCI DSS v3.2 Requirement 4.3