REQUIREMENT #1: INSTALL & MAINTAIN A FIREWALL CONFIGURATION TO PROTECT CARDHOLDER DATA

Firewalls are devices that control computer traffic allowed between City of Waukesha's networks and untrusted networks, as well as traffic into and out of more sensitive areas within City of Waukesha's internal trusted networks. The Cardholder Data Environment (CDE) is an example of a more sensitive area within City of Waukesha's trusted network. A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria.

All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employee Internet access through desktop browsers, employee e-mail access, dedicated connections such as business-to-business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network. Other system components may provide firewall functionality, provided they meet the minimum requirements for firewalls as provided in PCI DSS Requirement 1. Where other system components are used within the cardholder data environment to provide firewall functionality, these devices must be included within the scope and assessment of PCI DSS Requirement 1.

PCI DSS CONTROL 1.1

Control Objective: The organization establishes firewall and router configuration standards that follow industry-recognized leading practices.

Standard: Asset custodians are required to establish firewall and router configuration processes that include the following:[3]

(a) Asset custodians are required to establish and maintaining a formal process for approving and testing all network connections and changes to both firewall and router configurations;[4]

(b) Asset custodians are required to establish and maintaining detailed network diagrams. Network diagrams must:[5]
   1. Document all connections to cardholder data, including any wireless networks;
   2. Be reviewed annually; and
   3. Be updated as the network changes to reflect the current architecture in place;

(c) Asset custodians are required to establish and maintaining detailed data flow diagrams that show all cardholder data flows across systems and networks; A firewall is required to be installed at each Internet connection and between any Demilitarized Zone (DMZ) and City of Waukesha's internal networks;[6]

(d) All network devices must have a documented description of any applicable groups, roles, and responsibilities associated with the device to support configuration management and review processes;[7]

(e) A documented business justification is required for all services, protocols, ~~and~~ ports, and applications allowed through the firewall(s), including documentation of security features implemented for those protocols considered to be insecure;[8] and

(f) Firewall and router rule sets must be reviewed at least once every six (6) months and the review must cover:[9]
   1. ~~Validation of Access Control Lists (ACLs)~~Policies; and
   2. Vulnerability management (e.g., validating software and firmware is current).

Supplemental Guidance: Examples of insecure services, protocols, or ports include but are not limited to:

- File Transfer Protocol (FTP)
- Hypertext Transfer Protocol (HTTP)
- Internet Message Access Protocol (IMAP)

Procedures: Firewall rules are reviewed quarterly. All major changes follow Change Management procedures.

[3] PCI DSS v3.2 Requirement 1.1
[4] PCI DSS v3.2 Requirement 1.1.1
[5] PCI DSS v3.2 Requirement 1.1.2
[6] PCI DSS v3.2 Requirement 1.1.4
[7] PCI DSS v3.2 Requirement 1.1.5
[8] PCI DSS v3.2 Requirement 1.1.6
[9] PCI DSS v3.2 Requirement 1.1.7

PCI DSS CONTROL 1.2

Control Objective: The organization builds firewall and router configurations that restrict connections between untrusted networks and any system components in the Cardholder Data Environment (CDE).

Standard: Asset custodians are required to deploy and configure of firewalls and routers in order to restrict connections between untrusted networks and any system components within the Cardholder Data Environment (CDE) by the following means: [10]

(a) Implementing ~~Access Control Lists (ACLs)~~ Policies and other applicable filters to restrict the inbound and outbound traffic to the CDE to only that which is necessary, as defined by a business justification; [11]
(b) Securing and synchronizing router and firewall configuration files; [12] and
(c) Positioning perimeter firewalls between wireless networks and the CDE.[13]

PCI DSS CONTROL 1.3

Control Objective: The organization prohibits direct public access to the Internet and any system component in the Cardholder Data Environment (CDE).

Standard: Asset custodians are required to establish and manage firewall and router configuration standards to prohibit direct public access to the Internet and any system component in the Cardholder Data Environment (CDE) that includes, but is not limited to: [14]

(a) Demilitarized Zones (DMZ) are required to be implemented to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports; [15]
(b) Inbound Internet traffic shall be limited to IP addresses within the DMZ; [16]
(c) Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network; [17]
(d) Unauthorized outbound traffic from the CDE to the Internet are prohibited; [18]
(e) Stateful inspection (dynamic packet filtering) must be implemented; [19]
(f) System components that store cardholder data must be placed within an internal network zone, segregated from the DMZ and other untrusted networks; [20] and
(g) Private IP addresses and routing information are prohibited from being disclosed to unauthorized parties. [21]

Supplemental Guidance: A stateful firewall keeps track of the state of network connections (such as TCP streams or UDP communication) and is able to hold significant attributes of each connection in memory. These attributes are collectively known as the state of the connection, and may include such details as the IP addresses and ports involved in the connection and the sequence numbers of the packets traversing the connection. Stateful inspection monitors incoming and outgoing packets over time, as well as the state of the connection, and stores the data in dynamic state tables. This cumulative data is evaluated so that filtering decisions would not only be based on administrator-defined rules, but also on the context that has been built by previous connections as well as previous packets belonging to the same connection.

[10] PCI DSS v3.2 Requirement 1.2
[11] PCI DSS v3.2 Requirement 1.2.1
[12] PCI DSS v3.2 Requirement 1.2.2
[13] PCI DSS v3.2 Requirement 1.2.3
[14] PCI DSS v3.2 Requirement 1.3
[15] PCI DSS v3.2 Requirement 1.3.1
[16] PCI DSS v3.2 Requirement 1.3.2
[17] PCI DSS v3.2 Requirement 1.3.3
[18] PCI DSS v3.2 Requirement 1.3.4
[19] PCI DSS v3.2 Requirement 1.3.5
[20] PCI DSS v3.2 Requirement 1.3.6
[21] PCI DSS v3.2 Requirement 1.3.7

Methods to obscure IP addressing may include, but are not limited to:

- Network Address Translation (NAT)
- Placing servers containing cardholder data behind proxy servers/firewalls,
- Removal or filtering of route advertisements for private networks that employ registered addressing, or
- Internal use of RFC1918 address space instead of registered addresses.

PCI DSS CONTROL 1.4

Control Objective: The organization installs personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (e.g., laptops used by employees), which are used to access the organization's network.

Standard: Asset custodians are required to install and maintain firewall software or equivalent functionality on any Internet-accessible mobile device or computer which are used to access the Cardholder Data Environment (CDE) that includes, but is not limited to: [22]

(a) Firewall software must be configured by City of Waukesha's IT department;
(b) Configuration settings of the firewall software must not be alterable by standard users; and
(c) Firewall configurations must include:
    1. Specific configuration settings are defined for firewall software.
    2. Firewall software is actively running.
    3. Firewall software is not alterable by users of mobile devices and/or computers.

Supplemental Guidance: Examples of mobile devices and computers includes, but are not limited to:

- Laptops
- Tablets
- Smart phones

Procedures: The City uses NG Antivirus protection, which contains firewall rules and also works directly with the City's firewall.

PCI DSS CONTROL 1.5

Control Objective: Ensure that security policies and operational procedures for managing firewalls 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 managing firewalls are kept current and disseminated to all pertinent parties. [23]

Supplemental Guidance: Personnel need to be aware of and following security policies and operational procedures to ensure firewalls and routers are continuously managed to prevent unauthorized access to the network.

Procedures: The City IT department has a documentation Wiki where polices and procedures are stored.

[22] PCI DSS v3.2 Requirement 1.4
[23] PCI DSS v3.2 Requirement 1.5

REQUIREMENT #2: DO NOT USE VENDOR-SUPPLIED DEFAULTS FOR SYSTEM PASSWORDS & OTHER SECURITY PARAMETERS

Malicious individuals (external and internal to an organization) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known in hacker communities and are easily determined via public information.

PCI DSS CONTROL 2.1

Control Objective: The organization always changes vendor-supplied defaults before installing a system on the network.

Standard: Asset custodians are required to ensure vendor-supplied defaults are changed, prior to the information system being installed on the network. This pre-production hardening process for both wired and wireless information systems must include, but is not limited to: [24]

(a) Changing vendor default credentials: [25]
    1. Passwords;
    2. Simple Network Management Protocol (SNMP) community strings; and
    3. Encryption keys
(b) Disabling or deleting unnecessary accounts;
(c) Updating firmware on devices; and
(d) Verifying other security-related vendor defaults are changed, if applicable.

Supplemental Guidance: This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, Simple Network Management Protocol (SNMP) community strings, etc.) Use vendor manuals and sources on the Internet to find vendor-supplied accounts/passwords.

Procedures: This is a standard procedure.

PCI DSS CONTROL 2.2

Control Objective: The organization develops configuration standards for all system components that are consistent with industry-accepted system hardening standards.

Standard: Asset custodians are required to develop configuration standards for all system components that are consistent with industry-accepted system hardening standards. This process of pre-production hardening systems includes, but is not limited to: [26]

(a) Verifying that system configuration standards are:
    1. Updated as new vulnerability issues are identified;
    2. Applied when new systems are configured;
    3. Consistent with industry-accepted hardening standards;
(b) Implementing only one primary function per server to prevent functions that require different security levels from co-existing on the same server (e.g., web servers, database servers, and DNS should be implemented on separate servers); [27]
(c) Enforcing least functionality, which includes but is not limited to:
    1. Allowing only necessary and secure services, protocols, and daemons; [28]
    2. Removing all unnecessary functionality, which includes but is not limited to: [29]
        i. Scripts;
        ii. Drivers;
        iii. Features;
        iv. Subsystems;
        v. File systems; and
        vi. Unnecessary web servers
(d) Implementing security features for any required services, protocols or daemons that are considered to be insecure, which includes but is not limited to using secured technologies such as Secure Shell (SSH) v2 and higher, Secure File Transfer

[24] PCI DSS v3.2 Requirement 2.1
[25] PCI DSS v3.2 Requirement 2.1.1
[26] PCI DSS v3.2 Requirement 2.2
[27] PCI DSS v3.2 Requirement 2.2.1
[28] PCI DSS v3.2 Requirement 2.2.2
[29] PCI DSS v3.2 Requirement 2.2.5

Protocol (S-FTP), Transport Layer Security (TLS) v1.2 and higher, or IPSec VPN to protect insecure services such as NetBIOS, file-sharing, Telnet, and FTP; [30]

(e) Verifying system security parameters are configured to prevent misuse; [31] and

(f) Documenting the functionality present on information systems.

Supplemental Guidance: Appendix J: System Hardening contains the approved baseline configurations. Baseline configurations should be based on industry-recognized leading practices. Sources of approved baseline configurations are:

- Microsoft Security Configuration Wizard
- Center for Internet Security (CIS)
- Defense Cybersecurity Agency (DISA) Security Technical Implementation Guides (STIGs) [32]

If virtualization technologies are used, verify that only one primary function is implemented per virtual system component or device.

Procedures: This is defined in the Vulnerability Management Program. Please see the VMP document for details.

PCI DSS Control 2.3

Control Objective: The organization encrypts all non-console administrative access using strong cryptography.

Standard: Asset custodians are responsible for developing configuration standards to ensure all non-console administrative access is encrypting using strong cryptography using technologies such as SSH v2 and higher, VPN, or TLS v1.2 and higher for web-based management and other non-console administrative access. [33]

Supplemental Guidance: Examples of insecure services, protocols, or ports include but are not limited to:

- File Transfer Protocol (FTP);
- Telnet; and
- Post Office Protocol 3 (POP3).

Procedures: SSH v2 and higher, and TLS v1.2 and higher are the standards used by City IT.

PCI DSS Control 2.4

Control Objective: The organization maintains an inventory of system components that are in scope for PCI DSS.

Standard: Asset custodians are required to maintain an inventory of City of Waukesha's information systems that are in scope for PCI DSS and update the inventory at necessary. [34]

Supplemental Guidance: Maintaining a current list of all system components will enable City of Waukesha to accurately and efficiently define the scope of its CDE for implementing PCI DSS controls. Without an inventory, some system components could be forgotten, and be inadvertently excluded from applicable configuration standards.

Procedures: The inventory is maintained in our CMDB.

PCI DSS Control 2.5

Control Objective: The organization ensures that security policies and operational procedures for managing vendor defaults and other security parameters 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 managing vendor defaults and other security parameters are kept current and disseminated to all pertinent parties. [35]

[30] PCI DSS v3.2 Requirement 2.2.3
[31] PCI DSS v3.2 Requirement 2.2.4
[32] DISA STIGs official site: http://iase.disa.mil/stigs/index.html
[33] PCI DSS v3.2 Requirement 2.3
[34] PCI DSS v3.2 Requirement 2.4
[35] PCI DSS v3.2 Requirement 2.5

Supplemental Guidance: Personnel need to be aware of and following security policies and daily operational procedures to ensure vendor defaults and other security parameters are continuously managed to prevent insecure configurations.

Procedures: This is standard practice.

PCI DSS CONTROL 2.6

Control Objective: The organization's shared hosting providers protect the organization's hosted environment and cardholder data.

Standard: For shared hosting providers, City of Waukesha's contract owners, asset custodians and data owners are required to: [36]

(a) Maintain a comprehensive list of those service providers, including all applicable Service Level Agreements (SLAs);
(b) Require that providers of external information systems comply with City of Waukesha cybersecurity requirements and employ appropriate security controls in accordance with local, state and Federal laws, as well as all applicable regulatory requirements (e.g., PCI DSS);
(c) Define oversight responsibilities with regard to external information system services;
(d) Perform a review of the service provided for acceptable service levels;
(e) Conduct a risk assessment outsourcing of services; and
(f) Monitor security control compliance by those external service providers.

Supplemental Guidance: These providers must meet specific requirements as detailed in Appendix A (Additional PCI DSS Requirements for Shared Hosting Provider) of the PCI DSS.

Procedures: The City requires all hosting providers to provide their documentation annually.

[36] PCI DSS v3.2 Requirement 2.6

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~~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~~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

REQUIREMENT #5: USE & REGULARLY UPDATE ~~ANTI-VIRUS~~ENDPOINT PROTECTION SOFTWARE OR PROGRAMS

Malicious software, commonly referred to as "malware" (including viruses, worms, rootkits, and Trojans) enters network during many business-approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices. This can result in the exploitation of system vulnerabilities, so anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.

PCI DSS CONTROL 5.1

Control Objective: The organization deploys anti-malware software on systems commonly affected by malicious software.

Standard: Asset custodians are required to:

(a) Deploy the City of Waukesha-approved anti-malware software on all systems capable of running anti-malware software, including, but not limited to: [64]
    1. Workstations;
    2. Servers;
    3. Tablets;
    4. Mobile phones;

(b) Ensure that the City of Waukesha-approved anti-malware software is capable of detecting, removing, and protecting against all known types of malware; [65] and

(c) Perform periodic evaluations to identify and evaluate evolving malware threats on information systems considered to be not commonly affected by malware, in order to confirm whether such information systems continue to not require anti-malware software. [66]

Supplemental Guidance: Systems not capable of running anti-malware software should have a documented business justification as to why anti-malware software cannot be run and what compensating controls are in place to minimize the risk associated with the lack of anti-malware software on that system.

Typically, mainframes, mid-range computers (such as AS/400) and similar systems may not currently be commonly targeted or affected by malware. However, industry trends for malware can change quickly, so it is important for organizations to be aware of new malware that might affect their systems. For example, by monitoring vendor security notices and anti-malware newsgroups to determine whether their systems might be coming under threat from new and evolving malware.

Trends in malware should be included in the identification of new security vulnerabilities, and methods to address new trends should be incorporated into City of Waukesha's configuration standards and protection mechanisms as needed

Procedures: This is defined in the Vulnerability Management Program. Please see the VMP document for details.

PCI DSS CONTROL 5.2

Control Objective: The organization ensures that anti-malware mechanisms are current, actively running, and generating audit logs.

Standard: Asset custodians are required to ensure the City of Waukesha-approved anti-malware software is: [67]

(a) Kept current with updates from the anti-malware vendor;
(b) Actively running on systems the anti-malware software is deployed to; and
(c) Generating audit logs per PCI DSS requirement 10.7.

Supplemental Guidance: Even the best anti-malware solutions are limited in effectiveness if they are not maintained and kept current with the latest security updates, signature files, or malware protections. Audit logs provide the ability to monitor virus and malware activity and anti-malware reactions. Thus, it is imperative that anti-malware solutions be configured to generate audit logs and that these logs be managed in accordance with Requirement 10.

[64] PCI DSS v3.2 Requirement 5.1
[65] PCI DSS v3.2 Requirement 5.1.1
[66] PCI DSS v3.2 Requirement 5.1.2
[67] PCI DSS v3.2 Requirement 5.2

Procedures: Anti-malware test files from the European Institute for Computer Antivirus Research (EICAR) should be downloaded (http://www.eicar.org/85-0-Download.html) and copied to either a CD/DVD or write-protected USB.

- This CD/DVD or USB should be inserted into systems to test that anti-malware software is running "on demand" scans and detects the presence of the EICAR test file; and
- Logs should be checked to verify the EICAR test file was detected and logged.

PCI DSS CONTROL 5.3

Control Objective: The organization ensures that anti-malware mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.

Standard: Asset custodians are required to ensure the City of Waukesha-approved anti-malware software is actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.[68]

Supplemental Guidance: Anti-malware that continually runs and is unable to be altered will provide persistent security against malware. Use of policy-based controls on all systems to ensure anti-malware protections cannot be altered or disabled will help prevent system weaknesses from being exploited by malicious software. Additional security measures may also need to be implemented for the period of time during which anti-malware protection is not active (e.g., disconnecting the unprotected system from the Internet while the ~~anti-virus~~endpoint protection ~~protection~~ is disabled, and running a full scan after it is re-enabled).

Procedures: This is defined in the Vulnerability Management Program. Please see the VMP document for details.

PCI DSS CONTROL 5.4

Control Objective: The organization ensures that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.[69]

Standard: Asset custodians and data owners are required to ensure that the PCI DSS Cybersecurity Policy and appropriate standards and procedures for protecting systems against malware are kept current and disseminated to all pertinent parties.

Supplemental Guidance: Personnel need to be aware of and following security policies and operational procedures to ensure systems are protected from malware on a continuous basis.

Procedures: This is defined in the Vulnerability Management Program. Please see the VMP document for details.

[68] PCI DSS v3.2 Requirement 5.3
[69] PCI DSS v3.2 Requirement 5.4

REQUIREMENT #6: DEVELOP & MAINTAIN SECURE SYSTEMS & APPLICATIONS

Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Since many of these vulnerabilities are fixed by vendor-provided security patches, all critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.

PCI DSS CONTROL 6.1

Control Objective: The organization implements a process to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.

Standard: Asset custodians and data owners are required to rank vulnerabilities according to the National Vulnerability Database (NVD) Common Vulnerability Scoring System Support (CVSS) system. [70]

Supplemental Guidance: The NVD provides severity rankings of "Low," "Medium," and "High" in addition to the numeric CVSS scores.[71]

- Vulnerabilities are labeled "Low" severity if they have a CVSS base score of 0.0-3.9.
- Vulnerabilities will be labeled "Medium" severity if they have a base CVSS score of 4.0-6.9.
- Vulnerabilities will be labeled "High" severity if they have a CVSS base score of 7.0-10.0.

Procedures: This is defined in the Vulnerability Management Program. Please see the VMP document for details.

PCI DSS CONTROL 6.2

Control Objective: The organization ensures that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.

Standard: Asset custodians and data owners are required to ensure that: [72]

(a) All system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed;
(b) Critical security patches are installed within thirty (30) days of the vendor's release data; and
(c) Non-critical security patches are installed within ninety (90) days of the vendor's release data.

Supplemental Guidance: City of Waukesha is allowed to apply a risk-based approach to prioritize its patch installations. For example, by prioritizing critical infrastructure (e.g., public-facing devices and systems, databases) higher than less-critical internal devices, this helps ensure high-priority systems and devices are addressed within one month and still allows for addressing less critical devices and systems within three months.

Procedures: This is defined in the Vulnerability Management Program. Please see the VMP document for details.

PCI DSS CONTROL 6.3

Control Objective: The organization develops all internal and external software applications in accordance with PCI DSS and based on industry-recognized leading practices.

Standard: Contract owners, asset custodians, and data owners are required to ensure that internal and external developers:

(a) Develop software applications in accordance with PCI DSS and based on industry-recognized leading practices; [73]
(b) Incorporate cybersecurity throughout the software development lifecycle; [74]
(c) Remove custom application accounts, user IDs, and passwords before applications become active or are released to customers; [75] and
(d) Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated process) to include at least the following: [76]

[70] PCI DSS v3.2 Requirement 6.1
[71] National Vulnerability Database (NVD) Common Vulnerability Scoring System (CVSS) http://nvd.nist.gov/cvss.cfm
[72] PCI DSS v3.2 Requirement 6.2
[73] PCI DSS v3.2 Requirement 6.3
[74] PCI DSS v3.2 Requirement 6.3
[75] PCI DSS v3.2 Requirement 6.3.1
[76] PCI DSS v3.2 Requirement 6.3.2

1. Code changes must be reviewed by individuals other than the originating code author, and by individuals knowledgeable about code review techniques and secure coding practices;
2. Code reviews must ensure code is developed according to secure coding guidelines;
3. Appropriate corrections must be implemented prior to release; and
4. Code-review results must be reviewed and approved by management prior to release.

Supplemental Guidance: Secure coding guidelines are based on the Open Web Application Security Project (OWASP) guide.[77]

Procedures:

PCI DSS CONTROL 6.4

Control Objective: The organization follows change control processes and procedures for all changes to system components.

Standard: Asset custodians and data owners are required to follow change control processes and procedures for all changes to system components. The change control processes for assets within scope for PCI DSS include the following: [78]

(a) Utilize separate environments for development/testing/staging and production; [79]
(b) Utilize a separation of duties between development/testing/staging and production environments; [80]
(c) Prohibit the use of production data (e.g., live PANs) for testing or development; [81]
(d) Remove test data and accounts before production systems become active / goes into production; [82] and
(e) Develop change control procedures for the implementation of security patches and software modifications, which includes, but is not limited to the following: [83]
    1. Documentation of impact; [84]
    2. Documented change approval by authorized parties;[85]
    3. Functionality testing to verify that the change does not adversely impact the security of the system; [86] and
    4. Back-out procedures; [87] and
(f) Upon completion of significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable. [88]

Supplemental Guidance: Without properly documented and implemented change controls, security features could be inadvertently or deliberately omitted or rendered inoperable, processing irregularities could occur, or malicious code could be introduced.

Procedures: See ITCM-1.0 CHANGE MANAGEMENT POLICY for more details.

PCI DSS CONTROL 6.5

Control Objective: The organization develops applications based on secure coding guidelines.

Standard: Contract owners, asset custodians, and data owners are required to address common coding vulnerabilities in the software development process by ensuring the following:

(a) At least annually, developers are properly trained in current, secure coding techniques, including: [89]
    1. How to avoid common coding vulnerabilities, and
    2. Understanding how sensitive data is handled in memory
(b) Applications are developed based on secure coding guidelines: [90]

[77] Open Web Application Security Project (OWASP) Guide https://www.owasp.org
[78] PCI DSS v3.2 Requirement 6.4
[79] PCI DSS v3.2 Requirement 6.4.1
[80] PCI DSS v3.2 Requirement 6.4.2
[81] PCI DSS v3.2 Requirement 6.4.3
[82] PCI DSS v3.2 Requirement 6.4.4
[83] PCI DSS v3.2 Requirement 6.4.5
[84] PCI DSS v3.2 Requirement 6.4.5.1
[85] PCI DSS v3.2 Requirement 6.4.5.2
[86] PCI DSS v3.2 Requirement 6.4.5.3
[87] PCI DSS v3.2 Requirement 6.4.5.4
[88] PCI DSS v3.2 Requirement 6.4.6
[89] PCI DSS v3.2 Requirement 6.5
[90] PCI DSS v3.2 Requirement 6.5

1. Injection flaws, particularly SQL injection: [91]
    i. OS Command Injection;
    ii. LDAP and XPath injection flaws, and
    iii. Other forms of injection flaws;
2. Buffer overflow; [92]
3. Insecure cryptographic storage; [93]
4. Insecure communications; [94]
5. Improper error handling; [95]
6. All "High" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS requirement 6.1; [96]
7. Cross-site scripting (XSS); [97]
8. Improper access control, including but not limited to: [98]
    i. Insecure direct object references,
    ii. Failure to restrict URL access; and
    iii. Directory traversal;
9. Cross-site request forgery (CSRF); [99] and
10. Broken authentication and session management. [100]

Supplemental Guidance: Secure coding guidelines are based on the Open Web Application Security Project (OWASP) guide.[101]

Procedures: The City does not develop in-house applications that deal with cardholder data. The City staff that do application development do annual training that meets these requirements. ~~[insert a description of the actual procedures that you follow to meet this requirement]~~

PCI DSS CONTROL 6.6

Control Objective: The organization address new threats and vulnerabilities on an ongoing basis and ensure public-facing web applications are protected against known attacks.

Standard: Asset custodians and data owners are required to address public-facing web application threats and vulnerabilities by either of the following methods: [102]

(a) Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods:
    a. At least annually; and
    b. After any changes to the public facing website
(b) Installing an automated technical solution that detects and prevents web-based attacks (e.g., a web-application firewall) in front of public-facing web applications, to continually check all traffic.

Supplemental Guidance: Public-facing web applications are primary targets for attackers, and poorly coded web applications provide an easy path for attackers to gain access to sensitive data and systems. The requirement for reviewing applications or installing web-application firewalls is intended to reduce the number of compromises on public-facing web applications due to poor coding or application management practices.

- Manual or automated vulnerability security assessment tools or methods review and/or test the application for vulnerabilities

[91] PCI DSS v3.2 Requirement 6.5.1
[92] PCI DSS v3.2 Requirement 6.5.2
[93] PCI DSS v3.2 Requirement 6.5.3
[94] PCI DSS v3.2 Requirement 6.5.4
[95] PCI DSS v3.2 Requirement 6.5.5
[96] PCI DSS v3.2 Requirement 6.5.6
[97] PCI DSS v3.2 Requirement 6.5.7
[98] PCI DSS v3.2 Requirement 6.5.8
[99] PCI DSS v3.2 Requirement 6.5.9
[100] PCI DSS v3.2 Requirement 6.5.10
[101] Open Web Application Security Project (OWASP) Guide https://www.owasp.org
[102] PCI DSS v3.2 Requirement 6.6

- Web-application firewalls filter and block nonessential traffic at the application layer. Used in conjunction with a network-based firewall, a properly configured web-application firewall prevents application-layer attacks if applications are improperly coded or configured.

An organization that specializes in "application security" can be either a third-party company or an internal team/department, as long as the reviewers specialize in application security and can demonstrate independence from the development team.

Procedures: This is defined in the Vulnerability Management Program. Please see the VMP document for details.

PCI DSS CONTROL 6.7

Control Objective: The organization ensures that security policies and operational procedures for developing and maintaining secure systems and applications 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 developing and maintaining secure systems and applications are kept current and disseminated to all pertinent parties. [103]

Supplemental Guidance: Personnel need to be aware of and following security policies and operational procedures to ensure systems and applications are securely developed and protected from vulnerabilities on a continuous basis.

Procedures: The City does not develop in-house applications that deal with cardholder data. The City staff that develop applications do annual training that meets these requirements.

[103] PCI DSS v3.2 Requirement 6.7