PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS) CYBERSECURITY POLICY & STANDARDS

City of Waukesha

INTERNAL USE

Access Limited to Internal Use Only

TABLE OF CONTENTS

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS) POLICY OVERVIEW 5
INTRODUCTION 5
PURPOSE 5
SCOPE & APPLICABILITY 6
POLICY 6
VIOLATIONS 6
EXCEPTIONS 6
UPDATES 6
KEY TERMINOLOGY 7
CYBERSECURITY GOVERNANCE STRUCTURE 9
CYBERSECURITY CONSIDERATIONS FOR PROTECTING SYSTEMS 9
POLICIES, CONTROL OBJECTIVES, STANDARDS, PROCEDURES & GUIDELINES STRUCTURE 9
CYBERSECURITY CONTROLS 9
CYBERSECURITY PROGRAM ACTIVITIES 9
PCI DSS SECTION 1: BUILD & MAINTAIN A SECURE NETWORK 11
REQUIREMENT #1: INSTALL & MAINTAIN A FIREWALL CONFIGURATION TO PROTECT CARDHOLDER DATA 11
PCI DSS CONTROL 1.1 *11*
PCI DSS CONTROL 1.2 *12*
PCI DSS CONTROL 1.3 *12*
PCI DSS CONTROL 1.4 *13*
PCI DSS CONTROL 1.5 *13*
REQUIREMENT #2: DO NOT USE VENDOR-SUPPLIED DEFAULTS FOR SYSTEM PASSWORDS & OTHER SECURITY PARAMETERS 14
PCI DSS CONTROL 2.1 *14*
PCI DSS CONTROL 2.2 *14*
PCI DSS CONTROL 2.3 *15*
PCI DSS CONTROL 2.4 *15*
PCI DSS CONTROL 2.5 *15*
PCI DSS CONTROL 2.6 *16*
PCI DSS SECTION 2: PROTECT CARDHOLDER DATA 17
REQUIREMENT #3: PROTECT STORED CARDHOLDER DATA 17
PCI DSS CONTROL 3.1 *17*
PCI DSS CONTROL 3.2 *17*
PCI DSS CONTROL 3.3 *19*
PCI DSS CONTROL 3.4 *19*
PCI DSS CONTROL 3.5 *19*
PCI DSS CONTROL 3.6 *20*
PCI DSS CONTROL 3.7 *21*
REQUIREMENT #4: ENCRYPT TRANSMISSION OF CARDHOLDER DATA ACROSS OPEN, PUBLIC NETWORKS 21
PCI DSS CONTROL 4.1 *21*
PCI DSS CONTROL 4.2 *22*
PCI DSS CONTROL 4.3 *22*
PCI DSS SECTION 3: MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM 23
REQUIREMENT #5: USE & REGULARLY UPDATE ENDPOINT PROTECTION SOFTWARE OR PROGRAMS 23
PCI DSS CONTROL 5.1 *23*
PCI DSS CONTROL 5.2 *23*
PCI DSS CONTROL 5.3 *24*
PCI DSS CONTROL 5.4 *24*
REQUIREMENT #6: DEVELOP & MAINTAIN SECURE SYSTEMS & APPLICATIONS 25
PCI DSS CONTROL 6.1 *25*
PCI DSS CONTROL 6.2 *25*
PCI DSS CONTROL 6.3 *25*

PCI DSS Control 6.4 26
PCI DSS Control 6.5 26
PCI DSS Control 6.6 27
PCI DSS Control 6.7 28

PCI DSS Section 4: Implement Strong Access Control Measures 29

Requirement #7: Restrict Access To Cardholder Data By Business Need To Know 29
PCI DSS Control 7.1 29
PCI DSS Control 7.2 29
PCI DSS Control 7.3 30

Requirement #8: Assign A Unique ID To Each Person With Computer Access 30
PCI DSS Control 8.1 30
PCI DSS Control 8.2 31
PCI DSS Control 8.3 32
PCI DSS Control 8.4 32
PCI DSS Control 8.5 33
PCI DSS Control 8.6 33
PCI DSS Control 8.7 33
PCI DSS Control 8.8 ***Error! Bookmark not defined.***

Requirement #9: Restrict Physical Access To Cardholder Data – [Exempt. Do not store Cardholder Data] 35
PCI DSS Control 9.1 35
PCI DSS Control 9.2 35
PCI DSS Control 9.3 36
PCI DSS Control 9.4 36
PCI DSS Control 9.5 37
PCI DSS Control 9.6 37
PCI DSS Control 9.7 37
PCI DSS Control 9.8 38
PCI DSS Control 9.9 38
PCI DSS Control 9.10 39

PCI DSS Section 5: Regularly Monitor & Test Networks 40

Requirement #10: Track & Monitor All Access To Network Resources & Cardholder Data 40
PCI DSS Control 10.1 40
PCI DSS Control 10.2 40
PCI DSS Control 10.3 41
PCI DSS Control 10.4 41
PCI DSS Control 10.5 42
PCI DSS Control 10.6 42
PCI DSS Control 10.7 43
PCI DSS Control 10.8 43
PCI DSS Control 10.9 44

Requirement #11: Regularly Test Security Systems & Processes 44
PCI DSS Control 11.1 44
PCI DSS Control 11.2 44
PCI DSS Control 11.3 45
PCI DSS Control 11.4 46
PCI DSS Control 11.5 46
PCI DSS Control 11.6 46

PCI DSS Section 6: Maintain An Cybersecurity Policy 48

Requirement #12: Maintain A Policy That Addresses Cybersecurity For All Personnel 48
PCI DSS Control 12.1 48
PCI DSS Control 12.2 48
PCI DSS Control 12.3 48
PCI DSS Control 12.4 49
PCI DSS Control 12.5 49
PCI DSS Control 12.6 50
PCI DSS Control 12.7 50

PCI DSS Control 12.8 51
PCI DSS Control 12.9 51
PCI DSS Control 12.10 52
PCI DSS Control 12.11 52

Appendices 54
Appendix A: Data Classification & Handling Guidelines 54
A-1: Data Classification 54
A-2: Labeling 55
A-3: General Assumptions 55
A-4: Personally Identifiable Information (PII) 55
Appendix B: Data Classification Examples 58
Appendix C: Data Retention Periods 59
Appendix D: Cybersecurity Roles & Responsibilities 59
D-1: Cybersecurity Roles 59
D-2: Cybersecurity Responsibilities 59
Appendix E: Cybersecurity Exception Request Procedures 62
Appendix F: Types of Security Controls 63
F-1: Preventative Controls 63
F-2: Detective Controls 63
F-3: Corrective Controls 63
F-4: Recovery Controls 63
F-5: Directive Controls 63
F-6: Deterrent Controls 63
F-7: Compensating Controls 63
Appendix G: PCI DSS Self-Assessment Questionnaire (SAQ) 64
K-1: SAQ Overview 64
K-2: How To Determine Your SAQ 64

Glossary: Acronyms & Definitions 65
Acronyms 65
Definitions 65

Record of Changes 66

INTRODUCTION

The Payment Card Industry Data Security Standard (PCI DSS) Cybersecurity Policy & Standards document provides definitive information on the prescribed measures used to establish and enforce the cybersecurity program for PCI DSS v3.2 compliance at City of Waukesha (City of Waukesha).

City of Waukesha is committed to protecting its employees, partners, clients and City of Waukesha from damaging acts that are intentional or unintentional. Effective security is a team effort involving the participation and support of every City of Waukesha user who interacts with data and information systems. Therefore, it is the responsibility of every user to know this policy and to conduct their activities accordingly.

Protecting company information and the systems that collect, process, and maintain this information is of critical importance. Consequently, the security of information systems must include controls and safeguards to offset possible threats, as well as controls to ensure accountability, availability, integrity, and confidentiality of the data:

- Confidentiality – Confidentiality addresses preserving restrictions on information access and disclosure so that access is restricted to only authorized users and services.
- Integrity – Integrity addresses the concern that sensitive data has not been modified or deleted in an unauthorized and undetected manner.
- Availability – Availability addresses ensuring timely and reliable access to and use of information.

Security measures must be taken to guard against unauthorized access to, alteration, disclosure or destruction of cardholder data and information systems. This also includes against accidental loss or destruction.

PURPOSE

The purpose of this document is to prescribe a comprehensive framework for:

- Protecting the confidentiality, integrity, and availability of City of Waukesha's payment card data and related information systems.
- Protecting City of Waukesha, its employees, and its clients from illicit use of City of Waukesha's information systems and data.
- Ensuring the effectiveness of security controls over data and information systems that support City of Waukesha's operations.
- Recognizing the highly networked nature of the current computing environment and provide effective company-wide management and oversight of those related Cybersecurity risks.

The formation of the policy is driven by many factors, with the key factor being a risk. This policy sets the ground rules under which City of Waukesha shall operate and safeguard its data and information systems to both reduce risk and minimize the effect of potential incidents.

This policy, including related standards and procedures, are necessary to support the management of information risks in daily operations. The development of policy provides due care to ensure City of Waukesha users understand their day-to-day security responsibilities and the threats that could impact the company.

Implementing consistent security controls across the company will help City of Waukesha comply with current and future legal obligations to ensure long term due diligence in protecting the confidentiality, integrity, and availability of City of Waukesha data.

Scope & Applicability

This policy and its related standards, procedures, and guidelines apply to all City of Waukesha data, information systems, activities, and assets owned, leased, controlled, or used by City of Waukesha, its agents, contractors, or other business partners on behalf of City of Waukesha that are within scope of the PCI DSS. This policy applies to all City of Waukesha employees, contractors, sub-contractors, and their respective facilities supporting City of Waukesha business operations, wherever City of Waukesha data is stored or processed, including any third-party contracted by City of Waukesha to handle, process, transmit, store, or dispose of City of Waukesha data.

Some standards are explicitly stated for persons with a specific job function (e.g., a System Administrator); otherwise, all personnel supporting City of Waukesha business functions shall comply with the standards. City of Waukesha departments shall use this policy and its standards or may create a more restrictive set of policies and standards, but not one that is less restrictive, less comprehensive, or less compliant than this policy and its standards.

This policy and its standards do not supersede any other applicable law or higher-level company directive or existing labor management agreement in effect as of the effective date of this policy.

Appendix D: Cybersecurity Roles & Responsibilities provides a detailed description of City of Waukesha user roles and responsibilities, in regards to Cybersecurity.

City of Waukesha reserves the right to revoke, change, or supplement this policy and its standards, procedures, and guidelines at any time without prior notice. Such changes shall be effective immediately upon approval by management, unless otherwise stated.

Policy

City of Waukesha shall design, implement and maintain a coherent set of standards and procedures to manage risks to cardholder data, in an effort to ensure an acceptable level of Cybersecurity risk. Within the scope of the Cardholder Data Environment (CDE), City of Waukesha will protect and ensure the Confidentiality, Integrity, and Availability (CIA) of all its information systems and cardholder data, regardless of how it is created, distributed, or stored. Security controls will be tailored accordingly so that cost-effective controls can be applied commensurate with the risk and sensitivity of the data and information system. Security controls must be designed and maintained to ensure compliance with all legal requirements.

Violations

Any City of Waukesha user found to have violated any policy, standard, or procedure may be subject to disciplinary action, up to and including termination of employment. Violators of local, state, Federal, and/or international law may be reported to the appropriate law enforcement agency for civil and/or criminal prosecution.

Exceptions

While every exception to a policy or standard potentially weakens protection mechanisms for City of Waukesha information systems and underlying data, occasionally exceptions will exist. Procedures for requesting an exception to policies, procedures or standards are available in Appendix E: Cybersecurity Exception Request Procedures.

Updates

Updates to the PCI DSS Cybersecurity Policy will be announced to employees via management updates or email announcements. Changes will be noted in the Record of Changes to highlight the pertinent changes from the previous policies, standards, procedures, and guidelines.

KEY TERMINOLOGY

In the realm of cybersecurity terminology, the National Institute of Standards and Technology (NIST) IR 7298, Revision 1, *Glossary of Key Cybersecurity Terms*, is the primary reference document that City of Waukesha uses to define common cybersecurity terms. [1] Key terminology to be aware of includes:

Asset Custodian: A term describing a person or entity with the responsibility to assure that the assets are properly maintained, to assure that the assets are used for the purposes intended, and assure that information regarding the equipment is properly documented.

Cardholder Data Environment (CDE): A term describing the area of the network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment and thus the scope of the PCI assessment

Contract Owner: A term describing a person or entity that has been given formal responsibility for entering into and managing legal contracts with service providers. Contract owners are formally responsible for making sure due care and due diligence are performed by service providers, in regards to PCI DSS compliance.

Control: A term describing any management, operational, or technical method that is used to manage risk. Controls are designed to monitor and measure specific aspects of standards to help City of Waukesha accomplish stated goals or objectives. All controls map to standards, but not all standards map to Controls.

Control Objective: A term describing targets or desired conditions to be met that are designed to ensure that policy intent is met. Where applicable, Control Objectives are directly linked to an industry-recognized leading practice to align City of Waukesha with accepted due care requirements.

Data: A term describing an information resource that is maintained in electronic or digital format. Data may be accessed, searched, or retrieved via electronic networks or other electronic data processing technologies. Appendix A: Data Classification & Handling Guidelines provides guidance on data classification and handling restrictions.

Data Owner: A term describing a person or entity that has been given formal responsibility for the security of an asset, asset category, or the data hosted on the asset. It does not mean that the asset belongs to the owner in a legal sense. Asset owners are formally responsible for making sure that assets are secure while they are being developed, produced, maintained, and used.

Encryption: A term describing the conversion of data from its original form to a form that can only be read by someone that can reverse the encryption process. The purpose of encryption is to prevent unauthorized disclosure of data.

Guidelines: A term describing recommended practices that are based on industry-recognized leading practices. Unlike Standards, Guidelines allow users to apply discretion or leeway in their interpretation, implementation, or use.

Cybersecurity: A term that covers the protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. The focus is on the Confidentiality, Integrity, and Availability (CIA) of data.

Information System: A term describing an asset; a system or network that can be defined, scoped, and managed. Includes, but is not limited to, computers, workstations, laptops, servers, routers, switches, firewalls, and mobile devices.

Least Privilege: A term describing the theory of restricting access by only allowing users or processes the least set of privileges necessary to complete a specific job or function.

[1] NIST IR 7298 - http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Policy: A term describing a formally established requirement to guide decisions and achieve rational outcomes. Essentially, a policy is a statement of expectation that is enforced by standards and further implemented by procedures.

Procedure: A term describing an established or official way of doing something, based on a series of actions conducted in a certain order or manner. Procedures are the responsibility of the asset custodian to build and maintain, in support of standards and policies.

Sensitive Data: A term that covers categories of data that must be kept secure. Examples of sensitive data include Personally Identifiable Information, Payment Card Data (PCD), and all other forms of data classified as Restricted or Confidential in Appendix A: Data Classification & Handling Guidelines.

Service Provider: A term that includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. If a company provides a service that involves only the provision of public network access (such as a telecommunications company providing just the communication link) that entity would not be considered a service provider for that service (although they may be considered a service provider for other services).

Sensitive Personally Identifiable Information (PII): PII is commonly defined as the first name or first initial and last name, in combination with any one or more of the following data elements: [2]

- Social Security Number (SSN) / Taxpayer Identification Number (TIN) / National Identification Number (NIN)
- Driver License (DL) or another government-issued identification number (e.g., passport, permanent resident card, etc.)
- Financial account number
- Payment card number (e.g., credit or debit card)

Standard: A term describing formally established requirements in regard to processes, actions, and configurations.

[2] The source of this definition comes from two state laws - Oregon Consumer Identity Theft Protection Act - ORS 646A.600(11)(a) - http://www.leg.state.or.us/ors/646a.html and Massachusetts 201 CMR 17.00" Standards For The Protection of Personal Information of Residents of The Commonwealth - MA201CMR17.02 http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf

CYBERSECURITY CONSIDERATIONS FOR PROTECTING SYSTEMS

Appendix F: Type of Security Controls provides a detailed description of cybersecurity considerations in protecting information systems, based on the importance of the system and the sensitivity of the data processed or stored by the system.

POLICIES, CONTROL OBJECTIVES, STANDARDS, PROCEDURES & GUIDELINES STRUCTURE

Information security documentation is comprised of five main parts:

(1) Core policy that establishes management's intent;
(2) Control objective that identifies the condition that should be met;
(3) Standards that provides quantifiable requirements to be met;
(4) Procedures that establish how tasks must be performed to meet the requirements established in standards; and
(5) Guidelines are recommended, but not mandatory.

Figure 1: Policy Framework

CYBERSECURITY CONTROLS

Security controls are sometimes synonymous with standards, since controls are generally designed to directly map to standards. The PCI DSS Cybersecurity Policy security controls have a well-defined organization and structure, which supports ongoing compliance with the PCI DSS.

CYBERSECURITY PROGRAM ACTIVITIES

An Cybersecurity Management System (ISMS) focuses on cybersecurity management and IT-related risks. The governing principle behind City of Waukesha's ISMS is that, as with all management processes, the ISMS must remain effective and efficient in the long-term, adapting to changes in the internal organization and external environment.

In accordance with ISO/IEC 27001, City of Waukesha's ISMS incorporates the typical "Plan-Do-Check-Act" (PDCA), or Deming Cycle, approach:

- Plan: This phase involves designing the ISMS, assessing IT-related risks, and selecting appropriate controls.
- Do: This phase involves implementing and operating the appropriate security controls.
- Check: This phase involves reviewing and evaluating the performance (efficiency and effectiveness) of the ISMS.
- Act: This involves making changes, where necessary, to bring the ISMS back to optimal performance.

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, 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. 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 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 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 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.

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
- General Packet Radio Service (GPRS).

[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

Procedures: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.

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: 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

PCI DSS Section 3: Maintain A Vulnerability Management Program

Requirement #5: Use & Regularly Update 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 endpoint 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.

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
- 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.

---

[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

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

REQUIREMENT #7: RESTRICT ACCESS TO CARDHOLDER DATA BY BUSINESS NEED TO KNOW

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on the need to know and according to job responsibilities. "Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.

PCI DSS CONTROL 7.1

Control Objective: The organization limits access to system components and cardholder data to only those individuals whose job requires such access.

Standard: Asset custodians and data owners are required to implement administrative and technical measures to limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations include the following: [104]

(a) Defining access needs for each role, including: [105]
    1. System components and data resources that each role needs to access for their job function; and
    2. Level of privilege required (e.g., user, administrator, etc.) for accessing resources;
(b) Restricting access to privileged user IDs to least privileges necessary to perform job responsibilities; [106]
(c) Assigning access based on individual personnel's job classification and function; [107] and
(d) Requiring documented approval by authorized parties specifying required privileges. [108]

Supplemental Guidance: The implement of an automated access control system can be a combination of technology, since all modern computers, payment application, and Point of Sale (POS) software already have built-in systems for user accounts and privilege controls. Microsoft's PCI DSS Compliance Planning Guide should be referenced for using Active Directory as an automated access control system. [109]

Procedures: The City does not store cardholder data. It is explicitly prohibited by any department to store cardholder data physically or electronically. It is prohibited to process any "card not present" transaction via fax, email, or paper forms. It is strictly prohibited to store card holder data such as the Primary Account Number (PAN), security codes, or information on the magnetic strip (track 1 or 2) electronically or physically.

The City standard for access is the rule of least privilege: The Principle of Least Privilege states that a subject should be given only those privileges needed for it to complete its task. If a subject does not need an access right, the subject should not have that right.

PCI DSS CONTROL 7.2

Control Objective: The organization implements an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all," unless specifically allowed.

Standard: Asset custodians and data owners are required to ensure systems components are configured to restrict access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following: [110]

(a) Coverage of all system components; [111]
(b) Assignment of privileges to individuals based on job classification and function (RBAC); [112] and
(c) Default "deny-all" setting. [113]

---

[104] PCI DSS v3.2 Requirement 7.1
[105] PCI DSS v3.2 Requirement 7.1.1
[106] PCI DSS v3.2 Requirement 7.1.2
[107] PCI DSS v3.2 Requirement 7.1.3
[108] PCI DSS v3.2 Requirement 7.1.4
[109] Microsoft's Payment Card Industry Data Security Standard Compliance Planning Guide http://www.microsoft.com/en-us/download/details.aspx?id=18015
[110] PCI DSS v3.2 Requirement 7.2
[111] PCI DSS v3.2 Requirement 7.2.1
[112] PCI DSS v3.2 Requirement 7.2.2
[113] PCI DSS v3.2 Requirement 7.2.3

Supplemental Guidance: Without a mechanism to restrict access based on user's need to know, a user may unknowingly be granted access to cardholder data. An access control system automates the process of restricting access and assigning privileges. Additionally, a default "deny-all" setting ensures no one is granted access until and unless a rule is established specifically granting such access.

Vendor manuals should be used to validate setting, since some access control systems are set by default to "allow-all," thereby permitting access unless/until a rule is written to specifically deny it.

Procedures: This is standard practice with the door control system.

PCI DSS CONTROL 7.3

Control Objective: The organization ensures that security policies and operational procedures for restricting access to 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 restricting access to cardholder data are kept current and disseminated to all pertinent parties. [114]

Supplemental Guidance: Personnel need to be aware of and following security policies and operational procedures to ensure that access is controlled and based on need-to-know and least privilege, on a continuous basis.

Procedures: Policies are emailed and posted to the City's Intranet site. Policies are also distributed through the City's security awareness training system.

REQUIREMENT #8: ASSIGN A UNIQUE ID TO EACH PERSON WITH COMPUTER ACCESS

Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users. These requirements are applicable to all accounts, including Point of Sale (POS) accounts, with administrative capabilities and all accounts used to view or access cardholder data or to access systems with cardholder data.

PCI DSS CONTROL 8.1

Control Objective: The organization defines and implements policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components.

Standard: Asset custodians and data owners are required to assign all non-consumer users unique user identifications (ID) before allowing them to access system components. User identification controls include the following: [115]

(a) Controlling addition, deletion, and modification of user IDs, credentials, and other identifier objects; [116]
(b) Revoking access for any terminated users within twenty-four (24) hours of employment status change; [117]
(c) Removing or disabling inactive user accounts within ninety (90) days; [118]
(d) Managing user accounts assigned to vendors that are used to access, support, or maintain system components via remote access: [119]
    1. Enabling the accounts only during the time period needed and disabled when not in use; and
    2. Monitoring the accounts when in use;
(e) Limiting repeated access attempts be locked out after not more than six (6) invalid logon attempts; [120]
(f) Setting lockout durations to a minimum of thirty (30) minutes or until an administrator enables the user ID; [121] and

[114] PCI DSS v3.2 Requirement 7.3
[115] PCI DSS v3.2 Requirement 8.1, 8.1.1
[116] PCI DSS v3.2 Requirement 8.1.2
[117] PCI DSS v3.2 Requirement 8.1.3
[118] PCI DSS v3.2 Requirement 8.1.4
[119] PCI DSS v3.2 Requirement 8.1.5
[120] PCI DSS v3.2 Requirement 8.1.6
[121] PCI DSS v3.2 Requirement 8.1.7

(g) Require users to re-authenticate if a session has been idle for more than fifteen (15) minutes to re-activate the terminal or session. [122]

Supplemental Guidance: An example of uniqueness, the difference can be adding a designator to the end of the username, such as a number. Examples include:

- First user in the system named "John Smith": John.Smith or JSMITH
- Second user in the system named "John Smith": John.Smith1 or JSMITH1
- Third user in the system named "John Smith": John.Smith2 or JSMITH2

Procedures: This is standard practice, and the IT department has been working to eliminate any shared/generic user accounts. Any shared/generic user account that exists is locked down so that it can only perform the single function it is intended to.

PCI DSS CONTROL 8.2

Control Objective: The organization implements authentication mechanisms, in conjunction with unique IDs, to verify user legitimacy.

Standard: To ensure the proper management of user authentication for non-consumer users and administrators on all system components, user authentication mechanisms shall:

(a) Use at least one of the following methods to authenticate all users in addition to assigning a unique ID: [123]
    1. Something you know, such as a password or passphrase;
    2. Something you have, such as a token device or smart card; or
    3. Something you are, such as a biometric;
(b) Use strong cryptography to render all authentication credentials unreadable during transmission and storage; [124]
(c) Verifying user identity before modifying any authentication credential that includes, but is not limited to: [125]
    1. Performing password resets;
    2. Provisioning new tokens; or
    3. Generating new keys;
(d) Requiring complex passwords/phrases are used that contains: [126]
    1. A minimum length of at least seven (7) characters; and
    2. Both numeric and alphabetic characters;
(e) Forcing password/phrase changes at least once every ninety (90) days; [127] and
(f) Prohibiting individuals from submitting a new password/phrase that is the same as any of the last four (4) passwords/phrases he or she has used; and [128]
(g) Setting passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use. [129]

Supplemental Guidance: Since one of the first steps a malicious individual will take to compromise a system is to exploit weak or nonexistent passwords, it is important to implement good processes for authentication management. Passwords should never be written down or stored on-line in an unencrypted format.

Users must create passwords that can be easily remembered. One way to do this is to create a password based on a song title, affirmation, or another phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation. NOTE: Do not use either of these examples as passwords!

Strong (good) passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters (e.g., 0-9, !@#$%^&*)
- Eight (8) or more alphanumeric characters.
- Not a word in any language, slang, dialect, or jargon.

[122] PCI DSS v3.2 Requirement 8.1.8
[123] PCI DSS v3.2 Requirement 8.2
[124] PCI DSS v3.2 Requirement 8.2.1
[125] PCI DSS v3.2 Requirement 8.2.2
[126] PCI DSS v3.2 Requirement 8.2.3
[127] PCI DSS v3.2 Requirement 8.2.4
[128] PCI DSS v3.2 Requirement 8.2.5
[129] PCI DSS v3.2 Requirement 8.2.6

- Not based on personal information, names of family, or important calendar dates.

Weak (bad) passwords have the following characteristics:

- Default vendor password
- Contain less than seven (7) characters
- A word found in a dictionary (English or foreign)
- A common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
- The words "City of Waukesha" or any derivation.
- Birthdays and other personal information such as addresses and phone numbers.
- Word or number patterns (e.g., aaabbb, qwerty, zyxwvuts or 123321)
- Any of the above spelled backward.
- Any of the above preceded or followed by a digit (e.g., secret1 or 1secret)

City of Waukesha staff may perform password cracking on a periodic or random basis as part of the company's security testing procedures. If a password is guessed or cracked during one of these events, the user will be required to change it immediately.

Procedures: This is standard practice and is defined in the Default Domain Policy group policy object. The City IT implemented a Password Self-service Portal that has eliminated most password resets requests. When a password reset is requested City IT works directly with that user to enroll them in the portal.

PCI DSS CONTROL 8.3

Control Objective: The organization requires two-factor authentication for remote access originating from outside the Cardholder Data Environment (CDE) the by employees, administrators, and third parties.

Standard: Asset custodians are required to secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication: [130]

(a) Incorporate multi-factor authentication for all non-console access into the CDE for personnel with administrative access. [131]

(b) Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third-party access for support or maintenance) originating from outside City of Waukesha's network. [132]

Supplemental Guidance: If remote access is to City of Waukesha's network that has appropriate segmentation, such that remote users cannot access or impact the CDE, two-factor authentication for remote access to that non-CDE network would not be required. However, two-factor authentication is required for any remote access to networks with access to the CDE.

Examples of two-factor technologies include remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; and other technologies that facilitate two-factor authentication.

Procedures: The City does not store cardholder data, but does us multi-factor authentication for users who need remote connections via a VPN.

PCI DSS CONTROL 8.4

Control Objective: The organization documents and communicates authentication procedures and policies to all users.

Standard: In conjunction with the written policy and standards of the PCI DSS Cybersecurity Policy, managers and supervisors are required to provide their staff with: [133]

(a) Guidance on selecting strong authentication credentials;
(b) Guidance for how users should protect their authentication credentials;
(c) Instructions not to reuse previously used passwords;
(d) Instructions to change passwords if there is any suspicion the password could be compromised.

[130] PCI DSS v3.2 Requirement 8.3
[131] PCI DSS v3.2 Requirement 8.3.1
[132] PCI DSS v3.2 Requirement 8.3.2
[133] PCI DSS v3.2 Requirement 8.4

Supplemental Guidance: Personnel need to be aware of and following security policies, standards, and operational procedures to ensure account credentials are properly protected to prevent unauthorized access to the network.

Procedures: This is done during the onboarding process. Additionally, IT does send out an occasional email with tips, and reinforces this through the Security Awareness Training system.

PCI DSS CONTROL 8.5

Control Objective: The organization does not use group, shared, or generic IDs, passwords, or other generic authentication methods.

Standard: City of Waukesha's asset custodians and data owners are prohibited from using group, shared, or generic IDs, passwords, or other authentication methods as follows: [134]

(a) Generic user IDs must be disabled or removed;
(b) Shared user IDs must not exist for system administration and other critical functions;
(c) Shared and generic user IDs must not be used to administer any system components; and
(d) Service providers with remote access to customer premises (e.g., for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer. [135]

Supplemental Guidance: If multiple users share the same authentication credentials (e.g., user account and password), it becomes impossible to trace system access and activities to an individual. This, in turn, prevents an entity from assigning accountability for, or having effective logging off, an individual's actions, since a given action could have been performed by anyone in the group that has knowledge of the authentication credentials.

Procedures: This is standard practice, and the IT department has been working to eliminate any shared/generic user accounts. Any shared/generic user account that is locked down so that it can only perform the single function it is intended to.

PCI DSS CONTROL 8.6

Control Objective: The organization ensures authentication mechanisms are used (e.g., passwords, passphrases, physical or logical security tokens, smart cards, certificates, etc.) are assigned. [136]

Standard: Asset custodians must have mechanisms in place to attribute access to an individual and when non-traditional user authentication mechanisms are used (e.g., physical or logical security tokens, smart cards, certificates, etc.), the use of these mechanisms must be controlled, as follows:

(a) Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts.
(b) Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.

Supplemental Guidance: If user authentication mechanisms such as tokens, smart cards, and certificates can be used by multiple accounts, it may be impossible to identify the individual using the authentication mechanism. Having physical and/or logical controls (e.g., a PIN, biometric data, or a password) to uniquely identify the user of the account will prevent unauthorized users from gaining access through the use of a shared authentication mechanism.

Procedures: This is standard practice and is defined in the Default Domain Policy group policy object.

PCI DSS CONTROL 8.7

Control Objective: The organization ensures that access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted.

Standard: Data owners, in conjunction with asset custodians, are required to restrict all access to any database containing cardholder data (including access by applications, administrators, and all other users), as follows: [137]

(a) All user access to, user queries of, and user actions on databases must be through programmatic methods;

[134] PCI DSS v3.2 Requirement 8.5
[135] PCI DSS v3.2 Requirement 8.5.1
[136] PCI DSS v3.2 Requirement 8.6
[137] PCI DSS v3.2 Requirement 8.7

(b) Only database administrators may have the ability to directly access or query databases; and
(c) Application IDs for database applications may only be used by the applications (not by individual users or other non-application processes).

Supplemental Guidance: Without user authentication for access to databases and applications, the potential for unauthorized or malicious access increases, and such access cannot be logged since the user has not been authenticated and is therefore not known to the system. Also, database access should be granted through programmatic methods only (for example, through stored procedures), rather than via direct access to the database by end users (except for DBAs, who may need direct access to the database for their administrative duties).

Procedures: The City does not store cardholder data. However, the rule of least privilege is used when assigning permissions and allowing access to any system.

PCI DSS CONTROL 8.8

Control Objective: The organization ensures that security policies and operational procedures for identification and authentication 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 identification and authentication are kept current and disseminated to all pertinent parties. [138]

Supplemental Guidance: Personnel need to be aware of and following security policies and operational procedures for managing identification and authorization on a continuous basis.

Procedures: Policies are emailed and posted to the City's Intranet site. Policies are also distributed through the City's security awareness training system.

[138] PCI DSS v3.2 Requirement 8.8

REQUIREMENT #9: RESTRICT PHYSICAL ACCESS TO CARDHOLDER DATA – [EXEMPT. DO NOT STORE CARDHOLDER DATA]

Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hard copies, and should be appropriately restricted. For the purposes of Requirement 9, the following terminology applies:

- Onsite Personnel. This term refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity's premises.
- Visitor. This term refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day.
- Media. This term refers to all paper and electronic media containing cardholder data.
- Sensitive Area. This term refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.

PCI DSS CONTROL 9.1

Control Objective: The organization implements appropriate facility entry controls to limit and monitor physical access to systems in the Cardholder Data Environment (CDE).

Standard: Facility managers, in conjunction with asset custodians, are required to implement appropriate facility entry controls to limit and monitor physical access to systems in the CDE, including but not limited to: [139]

(a) Using video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries: [140]
    1. Video surveillance footage must be readily accessible for at least three (3) months, unless otherwise restricted by law; and
    2. Access control mechanisms (e.g., sign-in sheets) must be readily accessible for at least three (3) months;

(b) Restricting physical access to publicly accessible network jacks, by either: [141]
    1. Preventing physical access to the network jack; or
    2. Disconnecting unused or publicly accessible network jacks at the patch panel;

(c) Restricting physical access to Wireless Access Points (WAPs), gateways, handheld devices, networking/communications hardware, and telecommunication lines. [142]

Supplemental Guidance: Access control mechanisms may be as simple as a sign-in sheet to monitor individual access to sensitive areas, if video surveillance capabilities are not available.

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 9.2

Control Objective: The organization implements procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible.

Standard: Each department is responsible for developing procedures to easily distinguish between onsite personnel and visitors, including but is not limited to: [143]

(a) Identifying new onsite personnel or visitors (for example, assigning badges)
(b) Changes to access requirements
(c) Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).

Supplemental Guidance: Identifying authorized visitors so they are easily distinguished from onsite personnel prevents unauthorized visitors from being granted access to areas containing cardholder data.

[139] PCI DSS v3.2 Requirement 9.1
[140] PCI DSS v3.2 Requirement 9.1.1
[141] PCI DSS v3.2 Requirement 9.1.2
[142] PCI DSS v3.2 Requirement 9.1.3
[143] PCI DSS v3.2 Requirement 9.2

Procedures: Visitors entering secure areas, or areas where cardholder data is processed, need to have their visit logged, and wear a visitor's badge.

PCI DSS CONTROL 9.3

Control Objective: The organization implements physical access controls for onsite personnel to sensitive areas.

Standard: City of Waukesha's door control system allows each department to control maintain their own access control lists, except for City Hall. City Hall has multiple departments and the door system is administered by IT. Each department is responsible for controlling physical access for onsite personnel to the sensitive areas as follows: [144]

(a) Access must be authorized and based on individual job function.
(b) Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.

Supplemental Guidance: Controlling physical access to the CDE helps ensure that only authorized personnel with a legitimate business need are granted access. When personnel leave the organization, all physical access mechanisms should be returned or disabled promptly (as soon as possible) upon their departure, to ensure personnel cannot gain physical access to the CDE once their employment has ended.

Procedures: Each department that processes payments is responsible for getting the proper physical security in place and enforcing the standards and procedures in the policy document.

PCI DSS CONTROL 9.4

Control Objective: The organization implements procedures to identify, authorize and monitor visitors.

Standard: City of Waukesha's Information Technology department is responsible for implementing procedures to identify, authorize and monitor visitors as follows: [145]

(a) Visitors must be authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained; [146]
(b) Visitors must be identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel; [147]
(c) Visitors must be asked to surrender the badge or identification before leaving the facility or at the date of expiration; [148] and
(d) A visitor log must be used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted:[149]
    1. The log must include:
        i. The visitor's name;
        ii. The firm represented; and
        iii. The onsite personnel authorizing physical access on the log; and
    2. This log must be maintained for a minimum of three (3) months, unless otherwise restricted by law.

Supplemental Guidance: Visitor controls are important to reduce the ability of unauthorized and malicious persons to gain access to facilities (and potentially, to cardholder data). Visitor controls ensure visitors are identifiable as visitors so personnel can monitor their activities, and that their access is restricted to just the duration of their legitimate visit.

Procedures: The City's IT department uses a visitor management system that is available to all departments. As referenced elsewhere is this document, 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 including, but are not limited to facsimile

[144] PCI DSS v3.2 Requirement 9.3
[145] PCI DSS v3.2 Requirement 9.4
[146] PCI DSS v3.2 Requirement 9.4.1
[147] PCI DSS v3.2 Requirement 9.4.2
[148] PCI DSS v3.2 Requirement 9.4.3
[149] PCI DSS v3.2 Requirement 9.4.4

(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 9.5

Control Objective: The organization implements procedures to physically secure all media.

Standard: Data owners, in conjunction with asset custodians, are required to physically secure all media, as follows: [150]

(a) Store media back-ups in a secure location, preferably an off-site facility, such as: [151]
    1. An alternate or backup site; or
    2. A commercial storage facility; and
(b) Review the backup facility's security at least annually.

Supplemental Guidance: Controls for physically securing media are intended to prevent unauthorized persons from gaining access to cardholder data on any type of media. Cardholder data is susceptible to unauthorized viewing, copying, or scanning if it is unprotected while it is on removable or portable media, printed out, or left on someone's desk. Media includes but is not limited to computers, removable electronic media, paper receipts, paper reports, and faxes.

Procedures: The City's backup system does not store backups on removable media. Instead the backups are replicated to another secure facility electronically.

PCI DSS CONTROL 9.6

Control Objective: The organization maintains strict control over the internal or external distribution of any kind of media.

Standard: Data owners, in conjunction with asset custodians, are required to maintain strict control over the internal or external distribution of media, including the following: [152]

(a) Classifying media in accordance with Appendix A: Data Classification & Handling Guidelines so the sensitivity of the data can be determined; [153]
(b) Sending sensitive media by secured courier or another delivery method that can be accurately tracked; [154] and
(c) Ensuring prior management approval for any and all media that is moved from a secured area (including when media is distributed to individuals). [155]

Supplemental Guidance: Appendix A: Data Classification & Handling Guidelines covers the topics of data classification and handling in greater detail.

Procedures: It is strictly prohibited to store the contents of the payment card magnetic stripe (track data), The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever. It is also prohibited to store the PIN or the encrypted PIN Block under any circumstance.

PCI DSS CONTROL 9.7

Control Objective: The organization maintains strict control over the storage and accessibility of media.

Standard: Data owners, in conjunction with asset custodians, are required to:

(a) Maintain strict control over the storage and accessibility of media; [156]
(b) Properly maintain inventory logs of all media; [157] and
(c) Conduct media inventories at least annually. [158]

[150] PCI DSS v3.2 Requirement 9.5
[151] PCI DSS v3.2 Requirement 9.5.1
[152] PCI DSS v3.2 Requirement 9.6
[153] PCI DSS v3.2 Requirement 9.6.1
[154] PCI DSS v3.2 Requirement 9.6.2
[155] PCI DSS v3.2 Requirement 9.6.3
[156] PCI DSS v3.2 Requirement 9.7
[157] PCI DSS v3.2 Requirement 9.7.1
[158] PCI DSS v3.2 Requirement 9.7.1

Supplemental Guidance: Without careful inventory methods and storage controls, stolen or missing media could go unnoticed for an indefinite amount of time. If media is not inventoried, stolen or lost media may not be noticed for a long time or at all.

Procedures: It is strictly prohibited to store the contents of the payment card magnetic stripe (track data), The CVV/CVC (the 3 or 4 digit number on the signature panel on the reverse of the payment card) on any media whatsoever. It is also prohibited to store the PIN or the encrypted PIN Block under any circumstance.

PCI DSS CONTROL 9.8

Control Objective: The organization destroys media when it is no longer needed for business or legal reasons.

Standard: Data owners, in conjunction with asset custodians, are required to sanitize media when it is no longer needed for business or legal reasons. Asset custodians are required to destroy media that cannot be sanitized, as follows: [159]

(a) Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed; [160] or
    1. Secure storage containers must be used for cardholder data that is waiting to be destroyed.
(b) Render data on electronic media unrecoverable so that data cannot be reconstructed. [161]

Supplemental Guidance: Data destruction may be performed in-house, or it may be outsourced to a qualified data destruction vendor. Examples of methods for securely destroying electronic media include secure wiping, degaussing, or physical destruction (such as grinding or shredding hard disks).

Procedures: This is standard procedure, and the City uses a trusted vendor and receives documentation that the media has been destroyed.

PCI DSS CONTROL 9.9

Control Objective: The organization protects devices that capture payment card data via direct physical interaction with the card from tampering and substitution.

Standard: Facility managers, in conjunction with asset custodians and data owners, are required implement physical security controls and awareness training to protect devices that capture payment card data (e.g., Point of Sale (PoS) devices) via direct physical interaction with the card from tampering and substitution that includes, but is not limited to: [162]

(a) Maintaining an up-to-date list of devices that includes the following: [163]
    1. Make, model of device;
    2. Location of device (e.g., the address of the site or facility where the device is located); and
    3. Device serial number or another method of unique identification;
(b) Periodically inspecting device surfaces to detect tampering (e.g., addition of card skimmers to devices), or substitution (e.g., by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device); [164] and
(c) Providing training for personnel to be aware of attempted tampering or replacement of devices that includes the following: [165]
    1. Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices;
    2. Prohibiting the installation, replacement, or return devices without verification;
    3. Awareness for suspicious behavior around devices (e.g., attempts by unknown persons to unplug or open devices); and
    4. Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel (e.g., to a manager or security officer).

Supplemental Guidance: Criminals attempt to steal cardholder data by stealing and/or manipulating card-reading devices and terminals. For example, they will try to steal devices so they can learn how to break into them, and they often try to replace legitimate devices with fraudulent devices that send them payment card information every time a card is entered. Criminals will

[159] PCI DSS v3.2 Requirement 9.8
[160] PCI DSS v3.2 Requirement 9.8.1
[161] PCI DSS v3.2 Requirement 9.8.2
[162] PCI DSS v3.2 Requirement 9.9
[163] PCI DSS v3.2 Requirement 9.9.1
[164] PCI DSS v3.2 Requirement 9.9.2
[165] PCI DSS v3.2 Requirement 9.9.3

also try to add “skimming” components to the outside of devices, which are designed to capture payment card details before they even enter the device. For example, by attaching an additional card reader on top of the legitimate card reader so that the payment card details are captured twice: once by the criminal’s component and then by the device’s legitimate component. In this way, transactions may still be completed without interruption while the criminal is “skimming” the payment card information during the process. Additional best practices on skimming prevention are available on the PCI SSC website.

Procedures: Each department that processes payments is responsible for getting the proper physical security in place and enforcing the standards and procedures in the policy document.

PCI DSS CONTROL 9.10

Control Objective: The organization ensures that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties. [166]

Standard: Asset custodians and data owners are required to ensure that the PCI DSS Cybersecurity Policy and appropriate standards and procedures for restricting physical access to cardholder data are kept current and disseminated to all pertinent parties.

Supplemental Guidance: Personnel need to be aware of and following security policies and operational procedures for restricting physical access to cardholder data and CDE systems on a continuous basis.

Procedures: Each department that processes payments is responsible for getting the proper physical security in place, and enforcing the standards and procedures in the policy document.

[166] PCI DSS v3.2 Requirement 9.10

REQUIREMENT #10: TRACK & MONITOR ALL ACCESS TO NETWORK RESOURCES & CARDHOLDER DATA

Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

PCI DSS CONTROL 10.1

Control Objective: The organization implements audit trails for linking access to system components to individual users.

Standard: Asset custodians and data owners are required to implement auditing of systems and applications that allow access to system components to be linked to individual users. [167]

Supplemental Guidance: It is critical to have a process or system that links user access to system components accessed. This system generates audit logs and provides the ability to trace back suspicious activity to a specific user.

Procedures: This is accomplished using the City's Security Information and Event Management (SIEM) and system specific audit logs.

PCI DSS CONTROL 10.2

Control Objective: The organization utilizes automated audit trails for system components to reconstruct events.

Standard: Asset custodians and data owners are required to implement automated audit trails for all system components to reconstruct the following events: [168]

(a) All individual user accesses to cardholder data; [169]
(b) All actions taken by any individual with root or administrative privileges; [170]
(c) Access to all audit trails; [171]
(d) Invalid logical access attempts; [172]
(e) Use of and changes to identification and authentication mechanisms, including but not limited to: [173]
    1. creation of new accounts and elevation of privileges; and
    2. all changes, additions, or deletions to accounts with root or administrative privileges;
(f) Initialization, stopping, or pausing of the audit logs; [174] and
(g) Creation and deletion of system-level objects. [175]

Supplemental Guidance: Generating audit trails of suspect activities alerts the system administrator, sends data to other monitoring mechanisms (like intrusion detection systems), and provides a history trail for post-incident follow-up. Logging of the following events enables an organization to identify and trace potentially malicious activities.

Procedures: This is accomplished using the City's Security Information and Event Management (SIEM) and system specific audit logs.

[167] PCI DSS v3.2 Requirement 10.1
[168] PCI DSS v3.2 Requirement 10.2
[169] PCI DSS v3.2 Requirement 10.2.1
[170] PCI DSS v3.2 Requirement 10.2.2
[171] PCI DSS v3.2 Requirement 10.2.3
[172] PCI DSS v3.2 Requirement 10.2.4
[173] PCI DSS v3.2 Requirement 10.2.5
[174] PCI DSS v3.2 Requirement 10.2.6
[175] PCI DSS v3.2 Requirement 10.2.7

PCI DSS CONTROL 10.3

Control Objective: The organization follows best practices for logging audit trail entries.

Standard: Asset custodians and data owners are required to configure systems to record at least the following audit trail entries for all system components for each event: [176]

(a) User identification; [177]
(b) Type of event; [178]
(c) Date and time; [179]
(d) Success or failure indication; [180]
(e) Origination of event; [181] and
(f) Identity or name of affected data, system component, or resource. [182]

Supplemental Guidance: By recording these details for the auditable events at PCI DSS requirement 10.2, a potential compromise can be quickly identified, and with sufficient detail to know who, what, where, when, and how.

Procedures: This is accomplished using the City's Security Information and Event Management (SIEM) and system specific audit logs.

PCI DSS CONTROL 10.4

Control Objective: The organization utilizes time-synchronization technology to synchronize all critical system clocks.

Standard: Network Time Protocol (NTP) is City of Waukesha's official method of synchronizing all system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time:[183]

(a) Asset custodians are responsible for configuring City of Waukesha's NTP servers so that they are receiving time from industry-accepted time sources; [184] and
(b) Asset owners must ensure NTP on their systems is configured properly and validate the following:
    1. Systems are configured to synchronize time with City of Waukesha's NTP servers;
    2. Information systems have the correct and consistent time; [185] and
    3. Time data is protected from unauthorized modification. [186]

Supplemental Guidance: Time is commonly expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. NTP is an Internet standard protocol which enables client computers to maintain system time synchronization to the US Naval Observatory (USNO) Master Clocks in Washington, DC and Colorado Springs, CO.[187] Official NIST or USNO Internet Time Service (ITS) that can to be used for system time synchronization include, but are not limited to:

- time.nist.gov 192.43.244.18 [primary]; and
- time-nw.nist.gov 131.107.13.100 [alternate]

Procedures: All workstations and servers have their time synchronized with a domain controller; all other network devices use time.nist.gov

[176] PCI DSS v3.2 Requirement 10.3
[177] PCI DSS v3.2 Requirement 10.3.1
[178] PCI DSS v3.2 Requirement 10.3.2
[179] PCI DSS v3.2 Requirement 10.3.3
[180] PCI DSS v3.2 Requirement 10.3.4
[181] PCI DSS v3.2 Requirement 10.3.5
[182] PCI DSS v3.2 Requirement 10.3.6
[183] PCI DSS v3.2 Requirement 10.4
[184] PCI DSS v3.2 Requirement 10.4.3
[185] PCI DSS v3.2 Requirement 10.4.1
[186] PCI DSS v3.2 Requirement 10.4.2
[187] http://tycho.usno.navy.mil/ntp.html

PCI DSS CONTROL 10.5

Control Objective: The organization secures audit trails so logs cannot be altered.

Standard: Asset custodians and data owners are required to secure audit trails so the logs cannot be altered. Securing audit trails includes the following: [188]

(a) Limiting viewing of audit trails to those with a job-related need; [189]
(b) Protecting audit trail files from unauthorized modifications; [190]
(c) As close to real-time as possible, backup or transfer audit trail files to a centralized log server or media that is difficult to alter; [191]
(d) Writing logs for external-facing technologies onto a secure, centralized, internal log server or media device; [192] and
(e) Using File Integrity Monitoring (FIM) or change detection software on logs to ensure that existing log data cannot be changed without generating alerts. [193]

Supplemental Guidance: FIM or change detection software should be configured not to alert when new data is being added to logs. Otherwise normal log traffic will generate change alerts on the log files.

Procedures: Only network and system administrators have access to the City's Security Information and Event Management (SIEM) and system specific audit logs.

PCI DSS CONTROL 10.6

Control Objective: The organization implements a process to review logs and security events for all system components to identify anomalies or suspicious activity.

Standard: Asset custodians and data owners are required to develop and implement a process to review logs and security events for all system components to identify anomalies or suspicious activity that includes: [194]

(a) Reviewing the following, at least daily: [195]
    1. All security events;
    2. Logs of all system components that store, process, or transmit cardholder data, or that could impact the security of cardholder data;
    3. Logs of all critical system components; and
    4. Logs of all servers and system components that perform security functions. This includes, but is not limited to:
        i. Firewalls
        ii. Intrusion Detection Systems (IDS)
        iii. Intrusion Prevention Systems (IPS)
        iv. Authentication servers (e.g., Active Directory domain controllers); and
        v. E-commerce redirection servers;
(b) Reviewing logs of all other system components periodically based on City of Waukesha's policies and risk management strategy, as determined by City of Waukesha's annual risk assessment; [196] and
(c) Following up exceptions and anomalies identified during the review process. [197]

Supplemental Guidance: Many breaches occur over days or months before being detected. Checking logs daily minimizes the amount of time and exposure of a potential breach. Regular log reviews by personnel or automated means can identify and proactively address unauthorized access to the cardholder data environment.

The log review process does not have to be manual. The use of log harvesting, parsing, and alerting tools can help facilitate the process by identifying log events that need to be reviewed.

[188] PCI DSS v3.2 Requirement 10.5
[189] PCI DSS v3.2 Requirement 10.5.1
[190] PCI DSS v3.2 Requirement 10.5.2
[191] PCI DSS v3.2 Requirement 10.5.3
[192] PCI DSS v3.2 Requirement 10.5.4
[193] PCI DSS v3.2 Requirement 10.5.5
[194] PCI DSS v3.2 Requirement 10.6
[195] PCI DSS v3.2 Requirement 10.6.1
[196] PCI DSS v3.2 Requirement 10.6.2
[197] PCI DSS v3.2 Requirement 10.6.3

Procedures: This is accomplished using the City's Security Information and Event Management (SIEM) and system specific audit logs.

PCI DSS CONTROL 10.7

Control Objective: The organization retains audit trail history.

Standard: Asset custodians and data owners are required to retain audit trail history for at least one (1) year, with a minimum of three (3) months immediately available for analysis. [198]

Supplemental Guidance: Logs are considered "immediately available" for analysis if the logs can be:

- Accessed online;
- Readily recovered from archived media; or
- Restorable from back-up.

Procedures: This is accomplished using the City's Security Information and Event Management (SIEM) and system specific audit logs.

PCI DSS CONTROL 10.8

Control Objective: The organization is able to detect failures of critical security control systems in a timely manner.

Standard: Asset custodians and data owners are required to:

(a) Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: [199]
    1. Firewalls; IDS/IPS;
    2. FIM;
    3. Anti-malware;
    4. Physical access controls;
    5. Logical access controls;
    6. Audit logging mechanisms; and
    7. Segmentation controls (if used); and

(b) Develop processes for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: [200]
    1. Firewalls;
    2. IDS/IPS;
    3. FIM;
    4. Anti-malware;
    5. Physical access controls;
    6. Logical access controls;
    7. Audit logging mechanisms; and
    8. Segmentation controls (if used).

Supplemental Guidance: Without formal processes to detect and alert when critical security controls fail, failures may go undetected for extended periods and provide attackers ample time to compromise systems and steal sensitive data from the cardholder data environment.

The specific types of failures may vary depending on the function of the device and technology in use. Typical failures include a system ceasing to perform its security function or not functioning in its intended manner; for example, a firewall erasing all its rules or going offline.

Procedures: This is accomplished using the City's network monitoring system.

[198] PCI DSS v3.2 Requirement 10.7
[199] PCI DSS v3.2 Requirement 10.8
[200] PCI DSS v3.2 Requirement 10.8.1

PCI DSS CONTROL 10.9

Control Objective: The organization ensures that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties. [201]

Standard: Asset custodians and data owners are required to ensure that the PCI DSS Cybersecurity Policy and appropriate standards and procedures for monitoring all access to network resources and cardholder data are kept current and disseminated to all pertinent parties.

Supplemental Guidance: Personnel need to be aware of and following security policies and daily operational procedures for monitoring all access to network resources and cardholder data on a continuous basis.

Procedures: Policies are emailed and posted to the City's Intranet site. Policies are also distributed through the City's security awareness training system.

REQUIREMENT #11: REGULARLY TEST SECURITY SYSTEMS & PROCESSES

Vulnerabilities are being discovered continually by malicious individuals and are being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect the changing environment.

PCI DSS CONTROL 11.1

Control Objective: The organization implements processes to test for the presence of Wireless Access Points (WAPs) and detect and identify all authorized and unauthorized wireless access points.

Standard: Asset custodians are required to implement a process to test for the presence of Wireless Access Points (WAPs) that includes: [202]

(c) Detecting and identifying all authorized and unauthorized wireless access points at least once every ninety (90) days;
(d) Maintaining an inventory of authorized WAPs including a documented business justification; [203] and
(e) Implementing incident response procedures in the event unauthorized WAPs are detected. [204]

Supplemental Guidance: Detection methods must be sufficient to detect and identify both authorized and unauthorized devices. Methods that may be used in the rogue WAPs (802.11) detection process includes, but are not limited to:

- Wireless network scans,
- Physical/logical inspections of system components and infrastructure,
- Network Access Control (NAC); or
- Wireless Intrusion Detection Systems (IDS) / Intrusion Prevention Systems (IPS)

Procedures: The City's wireless access points detect rogue access points, and the WLAN controller alerts IT via email.

PCI DSS CONTROL 11.2

Control Objective: The organization implements a process for running internal and external network vulnerability scans at least quarterly and after any significant change in the network.

Standard: Asset custodians and data owners are required to perform the following vulnerability scanning-related activities: [205]

(a) Perform quarterly internal vulnerability scans and rescans as needed, until all "high-risk" vulnerabilities (as identified in Requirement 6.1) are resolved. Scans must be performed by qualified personnel; [206]
(b) Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans are achieved; [207] and

[201] PCI DSS v3.2 Requirement 10.9
[202] PCI DSS v3.2 Requirement 11.1
[203] PCI DSS v3.2 Requirement 11.1.1
[204] PCI DSS v3.2 Requirement 11.1.2
[205] PCI DSS v3.2 Requirement 11.2
[206] PCI DSS v3.2 Requirement 11.2.1
[207] PCI DSS v3.2 Requirement 11.2.2

(c) Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel. [208]

Supplemental Guidance: A "quarter" is defined as a ninety (90) day period and a "significant change" in the network includes, but is not limited to:

- New system component installations;
- Changes in network topology;
- Firewall rule modifications; and
- Major product upgrades.

Procedures: Vulnerability scans are performed weekly. See the Vulnerability and Patch Management Program document for more details.

PCI DSS CONTROL 11.3

Control Objective: The organization implements a methodology for penetration testing.

Standard: Asset custodians and data owners are required to implement a methodology for penetration testing that includes the following:

(a) Coverage of all PCI DSS version 3.0 requirements: [209]
    1. Process is based on industry-accepted penetration testing approaches (e.g., NIST SP 800-115);
    2. Includes coverage for the entire CDE perimeter and critical systems;
    3. Includes testing from both inside and outside the network;
    4. Includes testing to validate any segmentation and scope-reduction controls;
    5. Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in PCI DSS requirement 6.5;
    6. Defines network-layer penetration tests to include components that support network functions, as well as operating systems;
    7. Includes review and consideration of threats and vulnerabilities experienced in the last twelve (12) months; and
    8. Specifies retention of penetration testing results and remediation activities results.

(b) External penetration testing must be performed at least annually and after any significant infrastructure or application upgrade or modification. Examples include, but are not limited to: [210]
    1. An operating system upgrade;
    2. A sub-network added to the environment; or
    3. A web server added to the CDE;

(c) Internal penetration testing must be performed at least annually and after any significant infrastructure or application upgrade or modification. Examples include, but are not limited to: [211]
    1. An operating system upgrade;
    2. A sub-network added to the environment; or
    3. A web server added to the CDE;

(d) Exploitable vulnerabilities found during penetration testing must be corrected and testing shall be repeated to verify the corrections; [212] and

(e) If segmentation is used to isolate the CDE from other networks, penetration tests must be performed at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from in-scope systems. [213]

Supplemental Guidance: This update to PCI DSS requirement 11.3 is a best practice until June 30, 2015, after which it becomes a requirement. PCI DSS v2.0 requirements for penetration testing must be followed until v3.0 is in place.

Procedures: Penetration tests are performed annually. See the Vulnerability and Patch Management Program document for more details.

---

[208] PCI DSS v3.2 Requirement 11.2.3
[209] PCI DSS v3.2 Requirement 11.3
[210] PCI DSS v3.2 Requirement 11.3.1
[211] PCI DSS v3.2 Requirement 11.3.2
[212] PCI DSS v3.2 Requirement 11.3.3
[213] PCI DSS v3.2 Requirement 11.3.4 & 11.3.4.1

PCI DSS CONTROL 11.4

Control Objective: The organization utilizes intrusion-detection and/or intrusion prevention techniques to detect and/or prevent intrusions into the network.

Standard: Asset custodians and data owners are required to utilize Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS) to: [214]

(a) Prevent intrusions into the CDE;
(b) Monitor all traffic at the perimeter of the CDE, as well as at critical points in the CDE;
(c) Alert personnel to suspected compromises within the CDE; and
(d) Keep all intrusion-detection and prevention engines, baselines, and signatures up-to-date.

Supplemental Guidance: Intrusion detection and/or intrusion prevention techniques (such as IDS/IPS) compare the traffic coming into the network with known "signatures" and/or behaviors of thousands of compromise types (hacker tools, Trojans, and other malware), and send alerts and/or stop the attempt as it happens. Without a proactive approach to unauthorized activity detection, attacks on (or misuse of) computer resources could go unnoticed in real time. Security alerts generated by these techniques should be monitored so that the attempted intrusions can be stopped.

Procedures: The City's security fabric delivers broad protection and visibility to every network segment, device, appliance, whether virtual or physical. Both IDS and IPS are incorporated in the security fabric.

PCI DSS CONTROL 11.5

Control Objective: The organization deploys change-detection mechanisms to alert personnel to unauthorized modifications.

Standard: Asset custodians and data owners are required to deploy a change-detection mechanism (e.g., File Integrity Monitoring (FIM) tools) to: [215]

(a) Alert personnel to unauthorized modification of:
    1. Critical system files;
    2. Configuration files; or
    3. Content files;
(b) Configure the change-detection mechanism software to perform file comparisons at least weekly; and
(c) Implement a process to respond to any alerts generated by the change-detection mechanisms. [216]

Supplemental Guidance: For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come preconfigured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).
Examples of files that should be monitored:

- System executables;
- Application executables;
- Configuration and parameter files; and
- Centrally stored, historical or archived, log and audit files.

Procedures: The City uses several different products to accomplish this: Stealthbits, NetMon, and ADManager.

PCI DSS CONTROL 11.6

Control Objective: The organization ensures that security policies and operational procedures for security monitoring and testing 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 security monitoring and testing are kept current and disseminated to all pertinent parties. [217]

[214] PCI DSS v3.2 Requirement 11.4
[215] PCI DSS v3.2 Requirement 11.5
[216] PCI DSS v3.2 Requirement 11.5.1
[217] PCI DSS v3.2 Requirement 11.6

Supplemental Guidance: Personnel need to be aware of and following security policies and operational procedures for security monitoring and testing on a continuous basis.

Procedures: Policies are emailed and posted to the City's Intranet site.

PCI DSS Section 6: Maintain An Cybersecurity Policy

Requirement #12: Maintain A Policy That Addresses Cybersecurity For All Personnel

A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of Requirement 12, the term "personnel" refers to full-time and part-time employees, temporary employees, contractors and consultants who are resident on the entity's site or otherwise have access to the Cardholder Data Environment (CDE).

PCI DSS Control 12.1

Control Objective: The organization establishes, publishes, maintains and disseminates a security policy.

Standard: City of Waukesha's PCI DSS Cybersecurity Policy fulfills the requirement within PCI DSS for a security policy. City of Waukesha's management is responsible for the annual review of the PCI DSS Cybersecurity Policy, as well as updates, as necessary. [218]

Supplemental Guidance: A company's cybersecurity policy creates the roadmap for implementing security measures to protect its most valuable assets. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it.

Procedures: While, City of Waukesha's PCI DSS Cybersecurity Policy establishes the documentation requirement for PCI DSS, asset custodians, and data owners are required to:

- Review and update the PCI DSS Cybersecurity Policy, as needed; and
- Disseminate the PCI DSS Cybersecurity Policy to staff and subordinates to ensure all City of Waukesha personnel who interact with the CDE understand their requirements.

PCI DSS Control 12.2

Control Objective: The organization implements a risk-assessment process.

Standard: Asset custodians and data owners are required to implement a risk-assessment process that: [219]

(a) Is performed at least annually and upon significant changes to the environment (e.g., acquisition, merger, relocation);
(b) Identifies critical assets, threats, and vulnerabilities; and
(c) Results in a formal risk assessment.

Supplemental Guidance: Examples of risk assessment methodologies include but are not limited to

- OCTAVE;
- ISO 27005; and
- NIST SP 800-30.

Procedures: The City's IT department use the OCTAVE methodology for risk assessments. See the Vulnerability and Patch Management Program document for more details on identifying vulnerabilities.

PCI DSS Control 12.3

Control Objective: The organization develops and implements usage policies for critical technologies.

Standard: Asset custodians and data owners are required to develop and implement usage policies for critical technologies and defining the proper use of these technologies. Usage policies require the following: [220]

(a) Explicit approval by authorized parties; [221]
(b) Authentication for the use of the technology; [222]

[218] PCI DSS v3.2 Requirements 12.1, 12.1.1
[219] PCI DSS v3.2 Requirement 12.2
[220] PCI DSS v3.2 Requirement 12.3
[221] PCI DSS v3.2 Requirement 12.3.1
[222] PCI DSS v3.2 Requirement 12.3.2

(c) A list of all such devices and personnel with access; [223]
(d) A method to accurately and readily determine owner, contact information, and purpose (e.g., labeling, coding, and/or inventorying of devices); [224]
(e) Acceptable uses of the technology; [225]
(f) Acceptable network locations for the technologies; [226]
(g) List of company-approved products; [227]
(h) Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity; [228]
(i) Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use; [229] and
(j) For personnel accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. [230]

Supplemental Guidance: Appendix G: Rules of Behavior / User Acceptable Use covers City of Waukesha's rules of behavior. Examples of critical technologies include, but are not limited to:

- Remote-access technologies;
- Wireless technologies;
- Removable electronic media
- Laptops;
- Tablets;
- Smart phones;
- Personal data/digital assistants (PDAs),
- E-mail usage; and
- Internet usage.

Procedures: The Human Resource Department distributes the Acceptable Use Policy to all new hires.

PCI DSS Control 12.4

Control Objective: The organization defines cybersecurity responsibilities for all personnel. [231]

Standard: City of Waukesha's Human Resources (HR) department is required to ensure that cybersecurity policies, standards and procedures clearly define cybersecurity responsibilities for all personnel.

Supplemental Guidance: Cybersecurity roles and responsibilities are defined in Appendix D: Cybersecurity Roles & Responsibilities.

Procedures: Throughout 2019 and moving forward, IT policies will follow the approval procedure of ITB > Human Resource Committee > Common Council.

PCI DSS Control 12.5

Control Objective: The organization assigns an individual or a team cybersecurity management responsibilities.

Standard: City of Waukesha's assigned Information Security Officer (ISO) is required to perform or delegate the following cybersecurity management responsibilities: [232]

(a) Establish, document, and distribute security policies and procedures; [233]
(b) Monitor and analyze security alerts and information; [234]

[223] PCI DSS v3.2 Requirement 12.3.3
[224] PCI DSS v3.2 Requirement 12.3.4
[225] PCI DSS v3.2 Requirement 12.3.5
[226] PCI DSS v3.2 Requirement 12.3.6
[227] PCI DSS v3.2 Requirement 12.3.7
[228] PCI DSS v3.2 Requirement 12.3.8
[229] PCI DSS v3.2 Requirement 12.3.9
[230] PCI DSS v3.2 Requirement 12.3.10
[231] PCI DSS v3.2 Requirement 12.4 & 12.4.1
[232] PCI DSS v3.2 Requirement 12.5
[233] PCI DSS v3.2 Requirement 12.5.1
[234] PCI DSS v3.2 Requirement 12.5.2

(c) Distribute and escalate security alerts to appropriate personnel; [235]
(d) Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations; [236]
(e) Administer user accounts, including additions, deletions, and modifications; [237] and
(f) Monitor and control all access to data. [238]

Supplemental Guidance: Cybersecurity roles and responsibilities are defined in Appendix D: Cybersecurity Roles & Responsibilities.

Procedures: The City's IT Director fulfills the role of Information Security Officer.

PCI DSS CONTROL 12.6

Control Objective: The organization implements a formal security awareness program.

Standard: City of Waukesha's assigned Information Security Officer (ISO), in conjunction with City of Waukesha's Human Resources (HR) department, is required to develop and implement a formal security awareness program to make all personnel aware of the importance of cardholder data security, which includes: [239]

(a) Educating personnel upon hire and at least annually; [240] and
(b) Requiring applicable personnel to acknowledge at least annually that they have read and understood the PCI DSS Cybersecurity Policy and procedures. [241]

Supplemental Guidance: Awareness methods can vary depending on the role of the personnel and their level of access to the cardholder data. If personnel are not educated about their security responsibilities, security safeguards and processes that have been implemented may become ineffective through errors or intentional actions.

Requiring an acknowledgment by personnel in writing or electronically helps ensure that they have read and understood the security policies and that they have made and will continue to make a commitment to comply with these policies.

Procedures: The City's IT department has had a SAT Program in place since 2017, and City staff are run through training quarterly.

PCI DSS CONTROL 12.7

Control Objective: The organization screens potential personnel prior to hiring to minimize the risk of attacks from internal sources.

Standard: City of Waukesha's Human Resources (HR) department is responsible for screening potential personnel prior to hiring to minimize the risk of attacks from internal sources. [242]

Supplemental Guidance: For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only. Examples of background checks include, but are not limited to:

- Previous employment history;
- Criminal record;
- Credit history; and Reference checks.

Procedures: This has been a standard practice for a long time, and part of HR's role in the hiring process.

[235] PCI DSS v3.2 Requirement 12.5.2
[236] PCI DSS v3.2 Requirement 12.5.3
[237] PCI DSS v3.2 Requirement 12.5.4
[238] PCI DSS v3.2 Requirement 12.5.5
[239] PCI DSS v3.2 Requirement 12.6
[240] PCI DSS v3.2 Requirement 12.6.1
[241] PCI DSS v3.2 Requirement 12.6.2
[242] PCI DSS v3.2 Requirement 12.7

PCI DSS CONTROL 12.8

Control Objective: The organization maintains and implements policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data.

Standard: Contract owners, in conjunction with asset custodians and data owners, are required to maintain and implement policies and procedures to manage service providers that include, but is not limited to: [243]

(a) Maintaining a list of service providers; [244]
(b) Maintaining a written agreement that includes an acknowledgment that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of City of Waukesha, or to the extent that they could impact the security of City of Waukesha's CDE; [245]
(c) Ensures there is an established process for engaging service providers, including proper due diligence prior to engagement; [246]
(d) Maintaining a program to monitor service providers' PCI DSS compliance status at least annually; [247] and
(e) Maintaining information about which PCI DSS requirements are managed by each service provider, and which are managed by City of Waukesha. [248]

Supplemental Guidance: If the entity shares cardholder data with service providers (e.g., backup tape storage facilities, web hosting companies, or security service providers), the process of due diligence should include:

- Direct observations;
- Reviews of policies and procedures; and
- Reviews of supporting documentation.

Procedures: The City requires service providers to produce their compliance documents annually. Most service provider's documents are made available for download.

PCI DSS CONTROL 12.9

Control Objective: The organization ensures service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.

Standard: City of Waukesha's service providers are required to acknowledge in writing that they are responsible for the security of City of Waukesha's cardholder data that the service provider possesses or otherwise stores, processes, or transmits on behalf of City of Waukesha, or to the extent that they could impact the security of City of Waukesha's CDE. [249]

Supplemental Guidance: This requirement is a best practice until June 30, 2015, after which it becomes a requirement. The exact wording of acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The acknowledgment does not have to include the exact wording provided in this requirement.

Procedures: This is standard practice and a requirement of all service providers.

[243] PCI DSS v3.2 Requirement 12.8
[244] PCI DSS v3.2 Requirement 12.8.1
[245] PCI DSS v3.2 Requirement 12.8.2
[246] PCI DSS v3.2 Requirement 12.8.3
[247] PCI DSS v3.2 Requirement 12.8.4
[248] PCI DSS v3.2 Requirement 12.8.5
[249] PCI DSS v3.2 Requirements 12.9

PCI DSS CONTROL 12.10

Control Objective: The organization ensures an incident response capability exists and is prepared to respond immediately to potential cybersecurity incidents.

Standard: City of Waukesha's Incident Response (IR) team is required to:

(a) Implement an IR capability that is prepared to respond immediately to potential cybersecurity incidents. [250]
(b) Create an IR plan that is capable of being be implemented in the event of a system breach. Ensure the plan addresses the following, at a minimum: [251]
    1. Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum;
    2. Specific incident response procedures;
    3. Business recovery and continuity procedures;
    4. Data backup processes;
    5. Analysis of legal requirements for reporting compromises;
    6. Coverage and responses of all critical system components; and
    7. Reference or inclusion of incident response procedures from the payment brands.
(c) Test the IR plan at least annually; [252]
(d) Designate IR personnel to be available on a 24/7 basis to respond to alerts; [253]
(e) Provide appropriate training to staff with security breach response responsibilities; [254]
(f) Include alerts from security monitoring systems, including but not limited to: [255]
    1. Intrusion Detection Systems (IDS);
    2. Intrusion Prevention Systems (IPS);
    3. Firewalls; and
    4. File Integrity Monitoring (FIM) systems; and
(g) Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments. [256]

Supplemental Guidance: NIST guidance for incident response best practices can be referenced at:

- Computer Security Incident Handling Guide (http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf)
- Guide to Integrating Forensic Techniques into Incident Response (http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf)

Procedures: This is all defined in the Cyber Incident Response Plan (IRP), refer to the IRP for more details.

PCI DSS CONTROL 12.11

Control Objective: The organization ensures security control functionality by performing ongoing reviews of policies, standards, and procedures.

Standard: City of Waukesha's management is required to:

(a) Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes:
(b) Daily log reviews;
    1. Firewall ruleset reviews;
    2. Applying configuration standards to new systems;
    3. Responding to security alerts; and
    4. Change management processes;
(c) Maintain documentation of quarterly review process to include:
    1. Documenting results of the reviews; and
    2. Review and sign-off of results by personnel assigned responsibility for the PCI DSS compliance program.

[250] PCI DSS v3.2 Requirement 12.10
[251] PCI DSS v3.2 Requirement 12.10.1
[252] PCI DSS v3.2 Requirement 12.10.2
[253] PCI DSS v3.2 Requirement 12.10.3
[254] PCI DSS v3.2 Requirement 12.10.4
[255] PCI DSS v3.2 Requirement 12.10.5
[256] PCI DSS v3.2 Requirement 12.10.6

Supplemental Guidance: Regularly confirming that security policies and procedures are being followed provides assurance that the expected controls are active and working as intended. The objective of these reviews is not to re-perform other PCI DSS requirements, but to confirm whether procedures are being followed as expected.

The intent of these independent checks is to confirm whether security activities are being performed on an ongoing basis. These reviews can also be used to verify that appropriate evidence is being maintained—for example, audit logs, vulnerability scan reports, firewall reviews, etc.—to assist the entity's preparation for its next PCI DSS assessment.

Procedures: Policies are reviewed by the City of Waukesha Information Technology Board annually. The ITB can make recommendations for changes. After changes are approved, City IT staff review them and then update standard operating procedures accordingly. If polices effect City staff outside the IT department, IT emails the updated policy to everyone and then posts the updated policy on the City Intranet.

APPENDIX A: DATA CLASSIFICATION & HANDLING GUIDELINES

A-1: DATA CLASSIFICATION

Information assets are assigned a sensitivity level based on the appropriate audience for the information. If the information has been previously classified by regulatory, legal, contractual, or company directive, then that classification will take precedence. The sensitivity level then guides the selection of protective measures to secure the information. All data are to be assigned one of the following four sensitivity levels:

CLASSIFICATION	DATA CLASSIFICATION DESCRIPTION	
RESTRICTED	Definition	Restricted information is highly valuable, highly sensitive business information and the level of protection is dictated externally by legal and/or contractual requirements. Restricted information must be limited to only authorized employees, contractors, and business partners with a specific business need.
	Potential Impact of Loss	· **SIGNIFICANT DAMAGE** would occur if Restricted information were to become available to unauthorized parties either internal or external to City of Waukesha. · Impact could include negatively affecting City of Waukesha's competitive position, violating regulatory requirements, damaging the company's reputation, violating contractual requirements, and posing an identity theft risk.
CONFIDENTIAL	Definition	Confidential information is highly valuable, sensitive business information and the level of protection is dictated internally by City of Waukesha
	Potential Impact of Loss	· **MODERATE DAMAGE** would occur if Confidential information were to become available to unauthorized parties either internal or external to City of Waukesha. · Impact could include negatively affecting City of Waukesha's competitive position, damaging the company's reputation, violating contractual requirements, and exposing the geographic location of individuals.
INTERNAL USE	Definition	Internal Use information is information originated or owned by City of Waukesha, or entrusted to it by others. Internal Use information may be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the company's business interests.
	Potential Impact of Loss	· **MINIMAL or NO DAMAGE** would occur if Internal Use information were to become available to unauthorized parties either internal or external to City of Waukesha. · Impact could include damaging the company's reputation and violating contractual requirements.
PUBLIC	Definition	Public information is information that has been approved for release to the general public and is freely shareable both internally and externally.
	Potential Impact of Loss	· **NO DAMAGE** would occur if Public information were to become available to parties either internal or external to City of Waukesha. · Impact would not be damaging or a risk to business operations.

A-2: LABELING

Labeling is the practice of marking an information system or document with its appropriate sensitivity level so that others know how to appropriately handle the information. There are several methods for labeling information assets.

- **Printed**. Information that can be printed (e.g., spreadsheets, files, reports, drawings, or handouts) should contain one of the following confidentiality symbols in the document footer on every printed page (see below), or simply the words if the graphic is not technically feasible. The exception for labeling is with marketing material, since marketing material is primarily developed for public release.
- **Displayed**. Restricted or Confidential information that is displayed or viewed (e.g., websites, presentations, etc.) must be labeled with its classification as part of the display.

A-3: GENERAL ASSUMPTIONS

- Any information created or received by City of Waukesha employees in the performance of their jobs at is Internal Use, by default, unless the information requires greater confidentiality or is approved for release to the general public.
- Treat information that is not assigned a classification level as "Internal Use" at a minimum and use corresponding controls.
- When combining information with different sensitivity levels into a single application or database, assign the most restrictive classification of the combined asset. For example, if an application contains Internal Use and Confidential information, the entire application is Confidential.
- Restricted, Confidential and Internal Use information must never be released to the general public but may be shared with third parties, such as government agencies, business partners, or consultants, when there is a business need to do so and the appropriate security controls are in place according to the level of classification.
- You may not change the format or media of information if the new format or media you will be using does not have the same level of security controls in place. For example, you may not export Restricted information from a secured database to an unprotected Microsoft Excel spreadsheet.

A-4: PERSONALLY IDENTIFIABLE INFORMATION (PII)

Personally Identifiable Information (PII) is defined as the first name or first initial and last name, in combination with any one or more of the following data elements:

- Government-Issued Identification Number (e.g., passport, permanent resident card, etc.)
  - Social Security Number (SSN) / Taxpayer Identification Number (TIN) / National Identification Number (NIN)
  - Passport number
  - Permanent resident card
- Driver License (DL)
- Financial account number
  - Payment card number (credit or debit)
  - Bank account number
- Electronic Protected Health Information (ePHI)

A-5: DATA HANDLING GUIDELINES

HANDLING CONTROLS	RESTRICTED	CONFIDENTIAL	INTERNAL USE	PUBLIC
Non-Disclosure Agreement (NDA)	▪ NDA is required prior to access by non-City of Waukesha employees.	▪ NDA is recommended prior to access by non-City of Waukesha employees.	*No NDA requirements*	*No NDA requirements*
Internal Network Transmission (wired & wireless)	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited	▪ Encryption is recommended ▪ Instant Messaging is prohibited ▪ FTP is prohibited	*No special requirements*	*No special requirements*
External Network Transmission (wired & wireless)	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited ▪ Remote access should be used only when necessary and only with VPN and two-factor authentication	▪ Encryption is required ▪ Instant Messaging is prohibited ▪ FTP is prohibited	▪ Encryption is recommended ▪ Instant Messaging is prohibited ▪ FTP is prohibited	*No special requirements*
Data At Rest (file servers, databases, archives, etc.)	▪ Encryption is required ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific individuals	▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups	▪ Encryption is recommended ▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups	▪ Logical access controls are required to limit unauthorized use ▪ Physical access restricted to specific groups
Mobile Devices (iPhone, iPad, MP3 player, USB drive, etc.)	▪ Encryption is required ▪ Remote wipe must be enabled, if possible	▪ Encryption is required ▪ Remote wipe must be enabled, if possible	▪ Encryption is recommended ▪ Remote wipe should be enabled, if possible	*No special requirements*
Email (with and without attachments)	▪ Encryption is required ▪ Do not forward	▪ Encryption is required ▪ Do not forward	▪ Encryption is recommended	*No special requirements*
Physical Mail	▪ Mark "Open by Addressee Only" ▪ Use "Certified Mail" and sealed, tamper- resistant envelopes for external mailings ▪ Delivery confirmation is required ▪ Hand deliver internally	▪ Mark "Open by Addressee Only" ▪ Use "Certified Mail" and sealed, tamper- resistant envelopes for external mailings ▪ Delivery confirmation is required ▪ Hand delivering is recommended over interoffice mail	▪ Mail with company interoffice mail ▪ US Mail or other public delivery systems and sealed, tamper-resistant envelopes for external mailings	*No special requirements*
Printer	▪ Verify destination printer ▪ Attend printer while printing	▪ Verify destination printer ▪ Attend printer while printing	▪ Verify destination printer ▪ Retrieve printed material without delay	*No special requirements*

Web Sites	▪ Posting to intranet sites is prohibited, unless it is pre-approved to contain Restricted data. ▪ Posting to Internet sites is prohibited, unless it is pre-approved to contain Restricted data.	▪ Posting to publicly-accessible Internet sites is prohibited.	▪ Posting to publicly-accessible Internet sites is prohibited	*No special requirements*
Telephone	▪ Confirm participants on the call line ▪ Ensure private location	▪ Confirm participants on the call line ▪ Ensure private location	*No special requirements*	*No special requirements*
Video / Web Conference Call	▪ Pre-approve roster of attendees ▪ Confirm participants on the call line ▪ Ensure private location	▪ Pre-approve roster of attendees ▪ Confirm participants on the call line ▪ Ensure private location	▪ Pre-approve roster of attendees ▪ Confirm participants on the call line	*No special requirements*
Fax	▪ Attend receiving fax machine ▪ Verify destination number ▪ Confirm receipt ▪ Do not fax outside company without manager approval	▪ Attend receiving fax machine ▪ Verify destination number ▪ Confirm receipt ▪ Do not fax outside company without manager approval	*No special requirements*	*No special requirements*
Paper, Film/Video, Microfiche	▪ Return to owner for destruction ▪ Owner personally verifies destruction	▪ Shred or delete all documents or place in secure receptacle for future shredding	▪ Shred or delete all documents or place in secure receptacle for future shredding	*No special requirements*
Storage Media (Hard Disk Drives (HDDs), Flash drives, tapes, CDs/DVDs, etc.)	▪ Physically destroy the hard drives and media ▪ Requires use of company-approved vendor for destruction	▪ Physically destroy the hard drives and media or use commercial overwrite software to destroy the data on the media (quick reformat of the media is not sufficient)	▪ Physically destroy the hard drives and media or use commercial overwrite software to destroy the data on the media	▪ Physically destroy the hard drives and media or use commercial overwrite software to destroy the data on the media

APPENDIX B: DATA CLASSIFICATION EXAMPLES

The table below shows examples of common data instances that are already classified to simplify the process. This list is not inclusive of all types of data, but it establishes a baseline for what constitutes data sensitivity levels and will adjust to accommodate new types or changes to data sensitivity levels, when necessary.

IMPORTANT: You are instructed to classify data more sensitive than this guide, if you feel that is warranted by the content.

DATA CLASS	SENSITIVE DATA ELEMENTS	PUBLIC	INTERNAL USE	CONFIDENTIAL	RESTRICTED
Client or Employee Personal Data	Social Security Number (SSN)				X
	Employer Identification Number (EIN)				X
	Driver's License (DL) Number				X
	Financial Account Number				X
	Payment Card Number (credit or debit)				X
	Government-Issued Identification (e.g., passport, permanent resident card, etc.)				X
	Birth Date			X	
	First & Last Name		X		
	Age		X		
	Phone and/or Fax Number		X		
	Home Address		X		
	Gender		X		
	Ethnicity		X		
	Email Address		X		
Employee-Related Data	Compensation & Benefits Data				X
	Medical Data				X
	Workers Compensation Claim Data				X
	Education Data			X	
	Dependent or Beneficiary Data			X	
Sales & Marketing Data	Business Plan (including marketing strategy)			X	
	Financial Data Related to Revenue Generation			X	
	Marketing Promotions Development		X		
	Internet-Facing Websites (e.g., company website, social networks, blogs, promotions, etc.)	X			
	News Releases	X			
Networking & Infrastructure Data	Username & Password Pairs				X
	Public Key Infrastructure (PKI) Cryptographic Keys (public & private)				X
	Hardware or Software Tokens (multifactor authentication)				X
	System Configuration Settings			X	
	Regulatory Compliance Data			X	
	Internal IP Addresses			X	
	Privileged Account Usernames			X	
	Service Provider Account Numbers			X	
Strategic Financial Data	Corporate Tax Return Information			X	
	Legal Billings			X	
	Budget-Related Data			X	
	Unannounced Merger and Acquisition Information			X	
	Trade Secrets (e.g., design diagrams, competitive information, etc.)			X	
Operating Financial Data	Electronic Payment Information (Wire Payment / ACH)			X	
	Paychecks			X	
	Incentives or Bonuses (amounts or percentages)			X	
	Stock Dividend Information			X	
	Bank Account Information			X	
	Investment-Related Activity			X	
	Account Information (e.g., stocks, bonds, mutual funds, money markets, etc.)			X	
	Debt Amount Information			X	
	SEC Disclosure Information			X	

Appendix C: Data Retention Periods

See the City's record retention policy for retention periods.

Appendix D: Cybersecurity Roles & Responsibilities

D-1: Cybersecurity Roles

Every user at City of Waukesha, regardless of position or job classification, has an important role, when it comes to safeguarding the Confidentiality, Integrity, and Availability (CIA) of the information systems and data maintained by City of Waukesha. It is important that every individual fully understands their role, their associated responsibilities, and abide by the security standards, policies, and procedures set forth by the PCI DSS Cybersecurity Policy.

Role	Description of Security Role
Information Security Officer (ISO)	The ISO is accountable to the organization's senior management for the development and implementation of the cybersecurity program. The ISO will be the central point of contact for setting the day-to-day direction of the cybersecurity program and its overall goals, objectives, responsibilities, and priorities
Asset Owners	Business or department manager with budgetary authority over the system(s) with responsibility for the basic operation and maintenance of the system(s).
Asset Custodians	Under the direction of the ISO, asset custodians (e.g., system & network administrators) are responsible for the technical implementation and management of the PCI DSS Cybersecurity Policy. Party responsible for certain aspects of system security, such as adding and deleting user accounts, as authorized by the asset owner, as well as normal operations of the system in keeping with job requirements.
End Users	All employees (and contractors) are considered both custodians and users of the information systems and data on their issued information systems and are required to uphold all applicable PCI DSS Cybersecurity Policy policies, procedures, standards, and guidelines.

D-2: Cybersecurity Responsibilities

Responsibilities shall be assigned based on "ownership" or stake-holding by the Information Security Officer (ISO).

Role	Description of Security Responsibility
Company Management	▪ Oversee and approve the company's cybersecurity program; ▪ Appoint, in writing, an Information Security Officer (ISO) to implement the cybersecurity program; ▪ Ensure an appropriate level of protection for all company owned or maintained information resources; whether retained in-house or under the control of contractors; ▪ Ensure that funding and resources are programmed for staffing, training, and support of the cybersecurity program and for implementation of system safeguards, as required; ▪ Ensure that persons working in an cybersecurity role are properly trained, and supported with the appropriate resources; and ▪ Provide a secure processing environment including redundancy, backup, and fault-tolerance services.
Information Security Officer (ISO)	▪ Oversee and approve the company's cybersecurity program including the employees, contractors, and vendors who safeguard the company's information systems and data, as well as the physical security precautions for employees and visitors; ▪ Ensure an appropriate level of protection for the company's information resources; whether retained in-house or under the control of outsourced contractors; ▪ Issue the PCI DSS Cybersecurity Policy policies and guidance that establish a framework for an

	Cybersecurity Management System (ISMS); ▪ Identify protection goals, objectives, and metrics consistent with corporate strategic plan; ▪ Ensure appropriate procedures are in place for Security Testing & Evaluation (ST&E) for all information systems; and monitor, evaluate, and report to company management on the status of cybersecurity within the company; ▪ Ensure that persons working in an cybersecurity role are properly trained, and supported with the appropriate resources; ▪ Assist in compliance reviews and other reporting requirements; ▪ Provide feedback to company management on the status of the cybersecurity program, and suggest improvements or areas of concern in the program or any other security-related activity; ▪ Promote best practices in cybersecurity management; ▪ Monitor and evaluate the status of the company's cybersecurity posture by performing annual compliance reviews of the PCI DSS Cybersecurity Policy and system controls (including reviews of security plans, risk assessments, security testing processes, and others); ▪ Provide security-related guidance and technical assistance to all operating units; ▪ Develop the Computer Incident Response Program (CIRP) and act as the company's central point of contact for incident handling, in concert with the company's Computer Incident Response Team (CIRT). ▪ Maintain liaison with external organizations on security-related issues; ▪ Identify resource requirements, including funds, personnel, and contractors, needed to manage the cybersecurity program; and ▪ Assign ownership of resources.
Asset Owner	▪ Include security considerations in applications systems procurement or development, implementation, operation and maintenance, and disposal activities (e.g., life cycle management); ▪ Ensure the security of data and application software residing on system(s); ▪ Develop and maintain security plans and contingency plans for all general support systems and major applications under their responsibility, which document the business associations and dependencies of their system (e.g., examine linked IT resources and flow of information); ▪ Perform risk assessments to periodically re-evaluate sensitivity of the system, risks, and mitigation strategies; ▪ Conduct self-assessments of system safeguards and program elements and ensure certification and accreditation of the system; ▪ Report all incidents to the Computer Incident Response Team (CIRT) in a timely manner; ▪ Ensure system users have proper cybersecurity training (relevant to the system); ▪ Ensure IT contracts pertaining to the system include provisions for necessary security; ▪ Ensure that access to sensitive data is limited to those with a "need to know" or "need to use"; and ▪ Ensure systems' personnel are properly designated, monitored, and trained; ▪ Implement the system-level controls and maintain system documentation; ▪ Advise the system owner regarding security considerations in applications systems procurement or development, implementation, operation and maintenance, and disposal activities (e.g., life cycle management); ▪ Assist in the determination of an appropriate level of system and physical security commensurate with the level of sensitivity; ▪ Assist in the development and maintenance of security plans and contingency plans (e.g., Business Recovery Plans) for all general support systems and major applications under their responsibility; ▪ Participate in risk assessments to periodically re-evaluate sensitivity of the system, risks, and mitigation strategies; ▪ Participate in self-assessments of system safeguards and program elements and in certification and accreditation of the system; ▪ Attend security awareness training and programs; ▪ Maintain a cooperative relationship with business partners or other interconnected systems; ▪ Maintain an inventory of hardware and software; and ▪ Handle and investigate incidents in cooperation with and under direction of the Information Security Officer (ISO)

Asset Custodians (System & Network Administrators)	▪ Assist in the development and maintenance of security plans and contingency plans for all general support systems and major applications under their responsibility; ▪ Participate in risk assessments to periodically re-evaluate sensitivity of the system, risks, and mitigation strategies; ▪ Participate in self-assessments of system safeguards and program elements and in certification and accreditation of the system; ▪ Evaluate proposed technical security controls to assure proper integration with other system operations; ▪ Identify requirements for resources needed to effectively implement technical security controls; ▪ Ensure integrity in implementing and operating technical security controls; ▪ Report all incidents to the Computer Incident Response Team (CIRT) in a timely manner; ▪ Read and understand all applicable training and awareness materials; ▪ Read and understand all applicable use policies or other rules of behavior regarding use or abuse of company IT resources; ▪ Develop system administration and operational procedures and manuals; ▪ Evaluate and develop procedures that assure proper integration of service continuity with other system operations; ▪ Inventory those systems or parts of systems for which they are directly responsible (e.g., network equipment, servers, LAN, application administration, etc.); ▪ Know the sensitivity of the data they handle and take appropriate measures to protect it; and ▪ Know and abide by all applicable company policies and procedures.
End Users	NOTE: end user's responsibilities center upon being aware of the sensitivity and proper handling method of sensitive information. ▪ Know and abide by all applicable policies and procedures; ▪ Complete all required user training and awareness programs; ▪ Understand and abide by the Rules of Behavior (see Appendix G); ▪ Know which systems or parts of systems for which they are directly responsible (printer, desktop, browser, etc.); ▪ Know the sensitivity of the data handled by systems under your control and take appropriate measures to protect it; ▪ Report all incidents to the Computer Incident Response Team (CIRT) in a timely manner; ▪ Follow labeling, handling, sharing, storage and destruction requirements based on appropriate classification / sensitivity level; ▪ When in doubt about the classification of specific information, ask your supervisor; ▪ Comply with all regulatory, business or legal data retention policies before disposing of information.

APPENDIX E: CYBERSECURITY EXCEPTION REQUEST PROCEDURES

The following procedure defines the process for the review and approval of exceptions to the PCI DSS Cybersecurity Policy's policies, standards, guidelines, and procedures:

1. A manager (or an appointed designee) seeking an exception must assess the risks that non-compliance creates for the company. If the manager believes the risk is reasonable, then the manager prepares a written request describing the risk analysis and request for an exception (Note: The only reason to justify an exception is when compliance with a policy adversely affects business objectives or when the cost to comply offsets the risk of non-compliance). The risk analysis shall include:
    a. Identification of the threats and vulnerabilities, how likely each is to occur and the potential costs of an occurrence.
    b. The cost to comply.
2. Submit the request for an exception to the company's Information Security Officer (ISO is fulfilled by City's IT Director). The ISO will gather any necessary background information and make a recommendation to approve or deny the request. The ISO may recommend that other areas such as managers, asset custodians, and legal representatives review certain decisions.
3. The ISO will approve or deny the request for an exception.
4. The requestor will be notified of the decision to approve or deny.
5. All requests for exception will be retained by the ISO.
6. Exceptions are valid for a one-year period. Annually, the ISO will send a copy of approved exceptions back to the requestor, who must determine whether the conditions that justified the original exceptions are still in effect. If the conditions have substantially changed, a new request for exception must be submitted. Where little has changed, the review process may be shortened as recommended by the ISO.

APPENDIX F: TYPES OF SECURITY CONTROLS

F-1: PREVENTATIVE CONTROLS

Preventive security controls are put in place to prevent intentional or unintentional disclosure, alteration, or destruction of sensitive information. Examples include, but are not limited to:

- Policy - Unauthorized network connections are prohibited.
- Firewall - Blocks unauthorized network connections.
- Locked wiring closet - Prevents unauthorized equipment from being physically plugged into a network switch.

F-2: DETECTIVE CONTROLS

Detective security controls are like a burglar alarm. They detect and report an unauthorized or undesired event (or an attempted undesired event). Detective security controls are invoked after the undesirable event has occurred. Examples include, but are not limited to:

- Log monitoring and review – monitoring for anomalous traffic can detect unauthorized activity.
- System audit – monitoring for unauthorized changes can detect a breakdown in the change control process.
- File integrity checkers – monitoring for file changes can detect integrity compromises.
- Motion detection systems – monitoring for physical activity can detect a break in of a facility.

F-3: CORRECTIVE CONTROLS

Corrective security controls are used to respond to and fix a security incident. Corrective security controls also limit or reduce further damage from an attack. In many cases, the corrective security control is triggered by a detective security control. Examples include, but are not limited to:

- Procedures to clean a virus from an infected system.
- A guard checking and locking a door left unlocked by a careless employee.
- Updating firewall rules to block an attacking IP address as the attack is occurring.

F-4: RECOVERY CONTROLS

Recovery security controls are those controls that put a system back into production after an incident. Most Disaster Recovery activities fall into this category. Examples include, but are not limited to:

- After a disk failure, data is restored from a backup tape.
- A server automatically fails over to another server when a heartbeat (connectivity) is lost.

F-5: DIRECTIVE CONTROLS

Directive security controls are the equivalent of administrative controls. Directive controls dictate that some action is taken to protect sensitive organizational information. Examples include, but are not limited to:

- Policy, standards, procedures, or guidelines.
- HR handbook

F-6: DETERRENT CONTROLS

Deterrent security controls are controls that discourage security violations. Examples include, but are not limited to:

- An "Unauthorized Access Prohibited" sign may deter a trespasser from entering an area.
- The presence of security cameras might deter an employee from stealing equipment.
- A policy that states access to servers is monitored could deter unauthorized access.

F-7: COMPENSATING CONTROLS

Compensating security controls are controls that provide an alternative to normal controls that cannot be used for some reason. Examples include, but are not limited to:

- If a specific server cannot have antivirus software installed because it interferes with a critical application, a compensating control would be to increase monitoring of that server or isolate that server on its own network segment.
- If a system is not able to restrict who can log onto it, network segmentation would be a compensating control to protect the rest of the network from the lack of access control on the system.

APPENDIX G: PCI DSS SELF-ASSESSMENT QUESTIONNAIRE (SAQ)

K-1: SAQ OVERVIEW

For the authoritative reference, please go to: https://www.pcisecuritystandards.org/merchants/self_assessment_form.php

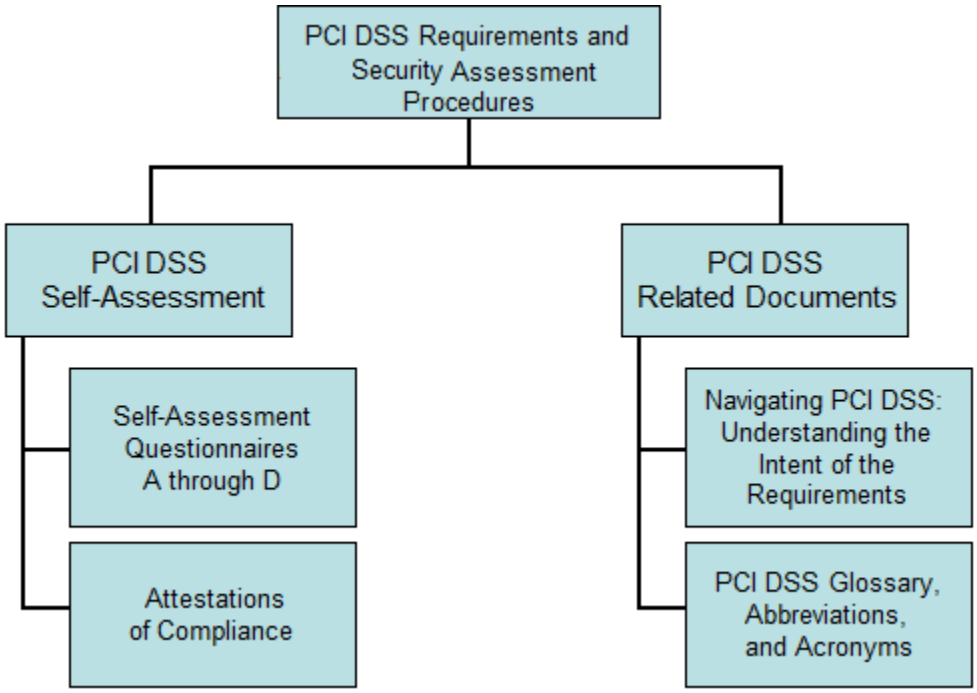
The PCI DSS SAQ is a validation tool for merchants and service providers that are not required to undergo an on-site data security assessment per the PCI DSS Security Assessment Procedures. The purpose of the SAQ is to assist organizations in self-evaluating compliance with the PCI DSS, and you may be required to share it with your acquiring bank. Please consult your acquirer for details regarding your PCI DSS validation requirements.

There are multiple versions of the PCI DSS SAQ to meet various business scenarios. A chart to help you determine which SAQ best applies to you and how to complete the SAQ is linked below, and is also included in the Instructions and Guidelines Document.

Each SAQ includes a series of yes-or-no questions about your security posture and practices. The SAQ allows for flexibility based on the complexity of a particular merchant's or service provider's business situation, as shown in the table below – this determines validation type. The SAQ validation type is not correlated with a merchant's classification or risk level.

Each Merchant must do the following three things:

- Be compliant with the entire PCI DSS 3.0 requirements;
- Perform a Self-Assessment Questionnaire (SAQ), based on their Merchant type; and
- Sign an Attestation of Compliance (AoC)



K-2: HOW TO DETERMINE YOUR SAQ

For the authoritative reference, please go to: https://www.pcisecuritystandards.org/minisite/en/saq-v3.0-documentation.php

GLOSSARY: ACRONYMS & DEFINITIONS

ACRONYMS

AD. Active Directory
APT. Advanced Persistent Threat
BCP. Business Continuity Plan
CDE. Cardholder Data Environment
CERT. Computer Emergency Response Team
CIRT. Computer Incident Response Team
COOP. Continuity of Operations Plan
CTI. Controlled Technical Information [257]
CUI. Controlled Unclassified Information [258]
DAC. Discretionary Access Control
DISA. Defense Information Security Agency
DLP. Data Loss Prevention
DRP. Disaster Recovery Plan
EAP. Extensible Authentication Protocol
EPHI. Electronic Protected Health Information
FICAM. Federal Identity, Credential, and Access Management
FIM. File Integrity Monitor
GDPR. General Data Protection Regulation
HIPAA. Health Insurance Portability and Accountability Act
IRP. Incident Response Plan
ISMS. Information Security Management System
ISO. International Organization for Standardization
LDAP. Lightweight Directory Authentication Protocol
MAC. Media Access Control
NIST. National Institute of Standards and Technology
PCI DSS. Payment Card Industry Data Security Standard
PDCA. Plan-Do-Check-Act
PIV. Personal Identity Verification
RBAC. Role-Based Access Control
TLS. Transport Layer Security

DEFINITIONS

City of Waukesha recognizes two sources for authoritative definitions:

- Payment Card Industry (PCI) Data Security Standard Glossary, Abbreviations and Acronyms. [259]
- Unified Compliance Framework (UCF) Compliance Library. [260]
- The National Institute of Standards and Technology (NIST) IR 7298, Revision 2, *Glossary of Key Information Security Terms*, is the approved reference document used to define common digital security terms. [261]

Security Requirements and Controls

The term control can be applied to a variety of contexts and can serve multiple purposes. When used in the security context, a security control can be a mechanism (i.e., a safeguard or countermeasure) designed to address protection needs that are specified by a set of security requirements.

- Controls are defined as the power to make decisions about how something is managed or how something is done; the ability to direct the actions of someone or something; an action, method, or law that limits; or a device or mechanism used to regulate or guide the operation of a machine, apparatus, or system.
- Requirements are defined as statements that translate or express a need and its associated constraints and conditions.[262]

[257] CUI Registry - https://www.archives.gov/cui/registry/category-detail/controlled-technical-info.html
[258] CUI Registry - https://www.archives.gov/cui/registry/category-list
[259] PCI Data Security Standard Glossary, Abbreviations and Acronyms - https://www.pcisecuritystandards.org/security_standards/glossary.php
[260] UCF Compliance Library - https://compliancedictionary.com
[261] NIST IR 7298 - http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf
[262] ISO/IEC/IEEE 29148

RECORD OF CHANGES

Issue	Date	Pages Affected	Description
Initial	TBD	All	Initial version. Complete rewrite for PCI DSS version 3.2
1.21	2/16/2021		See ITB Meeting minutes for changes during ITB meetings 10/7/20,11/4/20,12/2/20, and 1/6/21