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

City of Waukesha

TABLE OF CONTENTS

PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS) POLICY OVERVIEW 4
INTRODUCTION 4
PURPOSE 4
SCOPE & APPLICABILITY 5
POLICY 5
VIOLATIONS 5
EXCEPTIONS 5
UPDATES 5
KEY TERMINOLOGY 6
PCI DSS SECTION 1: BUILD & MAINTAIN A SECURE NETWORK 8
REQUIREMENT #1: INSTALL & MAINTAIN A FIREWALL CONFIGURATION TO PROTECT CARDHOLDER DATA 8
PCI DSS CONTROL 1.1 8
PCI DSS CONTROL 1.2 8
PCI DSS CONTROL 1.3 8
PCI DSS CONTROL 1.4 8
PCI DSS CONTROL 1.5 8
REQUIREMENT #2: DO NOT USE VENDOR-SUPPLIED DEFAULTS FOR SYSTEM PASSWORDS & OTHER SECURITY PARAMETERS 8
PCI DSS CONTROL 2.1 8
PCI DSS CONTROL 2.2 8
PCI DSS CONTROL 2.3 9
PCI DSS CONTROL 2.4 9
PCI DSS CONTROL 2.5 9
PCI DSS CONTROL 2.6 9
PCI DSS SECTION 2: PROTECT CARDHOLDER DATA 9
REQUIREMENT #3: PROTECT STORED CARDHOLDER DATA 9
REQUIREMENT #4: ENCRYPT TRANSMISSION OF CARDHOLDER DATA ACROSS OPEN, PUBLIC NETWORKS 9
PCI DSS CONTROL 4.1 9
PCI DSS CONTROL 4.2 9
PCI DSS CONTROL 4.3 9
PCI DSS SECTION 3: MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM 9
REQUIREMENT #5: USE & REGULARLY UPDATE ENDPOINT PROTECTION SOFTWARE OR PROGRAMS 9
REQUIREMENT #6: DEVELOP & MAINTAIN SECURE SYSTEMS & APPLICATIONS 9
PCI DSS SECTION 4: IMPLEMENT STRONG ACCESS CONTROL MEASURES 9
REQUIREMENT #7: RESTRICT ACCESS TO CARDHOLDER DATA BY BUSINESS NEED TO KNOW 10
PCI DSS CONTROL 7.1 10
PCI DSS CONTROL 7.2 10
PCI DSS CONTROL 7.3 10
REQUIREMENT #8: ASSIGN A UNIQUE ID TO EACH PERSON WITH COMPUTER ACCESS 10
PCI DSS CONTROL 8.1 10
PCI DSS CONTROL 8.2 10
PCI DSS CONTROL 8.3 10
PCI DSS CONTROL 8.4 10
PCI DSS CONTROL 8.5 10
PCI DSS CONTROL 8.6 11
PCI DSS CONTROL 8.7 11
PCI DSS CONTROL 8.8 11
REQUIREMENT #9: RESTRICT PHYSICAL ACCESS TO CARDHOLDER DATA – [EXEMPT. DO NOT STORE CARDHOLDER DATA] 11
PCI DSS CONTROL 9.1 11
PCI DSS CONTROL 9.2 11
PCI DSS CONTROL 9.3 11
PCI DSS CONTROL 9.4 11

PCI DSS Control 9.5 11
PCI DSS Control 9.6 11
PCI DSS Control 9.7 12
PCI DSS Control 9.8 12
PCI DSS Control 9.9 12
PCI DSS Control 9.10 12

PCI DSS Section 5: Regularly Monitor & Test Networks 12

Requirement #10: Track & Monitor All Access To Network Resources & Cardholder Data 12

Requirement #11: Regularly Test Security Systems & Processes 12

PCI DSS Control 11.1 12
PCI DSS Control 11.2 12
PCI DSS Control 11.3 12
PCI DSS Control 11.4 12
PCI DSS Control 11.5 13
PCI DSS Control 11.6 13

PCI DSS Section 6: Maintain An Cybersecurity Policy 13

Requirement #12: Maintain A Policy That Addresses Cybersecurity For All Personnel 13

PCI DSS Control 12.1 13
PCI DSS Control 12.2 13
PCI DSS Control 12.3 13
PCI DSS Control 12.4 13
PCI DSS Control 12.5 13
PCI DSS Control 12.6 13
PCI DSS Control 12.7 13
PCI DSS Control 12.8 13
PCI DSS Control 12.9 14
PCI DSS Control 12.10 14
PCI DSS Control 12.11 14

Appendices 15

Appendix A: Data Classification & Handling Guidelines 15

A-1: Data Classification 15
A-2: Labeling 16
A-3: General Assumptions 16
A-4: Personally Identifiable Information (PII) 16

Appendix B: Data Retention Periods 19

Appendix C: Cybersecurity Roles & Responsibilities 19

C-1: Cybersecurity Roles 19
C-2: Cybersecurity Responsibilities 19

Record of Changes 22

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 v4 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.

Payment Card Industry Data Security Standard Self-Assessment Surveys (PCI DSS SAQ) allow merchants, service providers, and other businesses to assess every aspect of their security in terms of PCI DSS compliance requirements. The City is Self-Assessed at SAQ B-IP.

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

PCI DSS Section 1: Build & Maintain A Secure Network

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.

Procedures:
The City follows industry standards with our firewall configuration.

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).

Procedures: Credit card readers are on their own VLAN.

PCI DSS Control 1.3

Procedures: Credit card readers are on their own VLAN

PCI DSS Control 1.4

The City is SAQ B-IP, and this control does not apply.

PCI DSS Control 1.5

The City is SAQ B-IP, and this control does not apply.

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.

Procedures: This is a standard procedure.

PCI DSS Control 2.2

The City is SAQ B-IP, and this control does not apply.

PCI DSS Control 2.3
Control Objective: The organization encrypts all non-console administrative access using strong cryptography.

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

PCI DSS Control 2.4
The City is SAQ B-IP, and this control does not apply.

PCI DSS Control 2.5
The City is SAQ B-IP, and this control does not apply.

PCI DSS Control 2.6
The City is SAQ B-IP, and this control does not apply.

PCI DSS Section 2: Protect Cardholder Data

Requirement #3: Protect Stored Cardholder Data
The City is SAQ B-IP, and this requirement does not apply.

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.

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.

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
The City is SAQ B-IP, and this control does not apply.

PCI DSS Section 3: Maintain A Vulnerability Management Program

---

Requirement #5: Use & Regularly Update Endpoint protection Software or Programs
The City is SAQ B-IP, and this requirement does not apply.

Requirement #6: Develop & Maintain Secure Systems & Applications
The City does not develop in-house applications that deal with cardholder data, and the development requirements do not apply. All other controls can be found in Vulnerability Management Program. Please see the VMP document for details.

PCI DSS Section 4: Implement Strong Access Control Measures

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.

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

The City is SAQ B-IP, and this control does not apply.

PCI DSS Control 7.3

The City is SAQ B-IP, and this control does not apply.

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.

Procedures: This is standard practice.

PCI DSS Control 8.2

The City is SAQ B-IP, and this control does not apply.

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.

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

PCI DSS Control 8.4

The City is SAQ B-IP, and this control does not apply.

PCI DSS Control 8.5

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

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
The City is SAQ B-IP, and this control does not apply.

PCI DSS Control 8.7
The City is SAQ B-IP, and this control does not apply.

PCI DSS Control 8.8
The City is SAQ B-IP, and this control does not apply.

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).

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
The City is SAQ B-IP, and this control does not apply.

PCI DSS Control 9.3
The City is SAQ B-IP, and this control does not apply.

PCI DSS Control 9.4
The City is SAQ B-IP, and this control does not apply.

PCI DSS Control 9.5
Control Objective: The organization implements procedures to physically secure all media.

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.

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.

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.

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.

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
The City is SAQ B-IP, and this control does not apply.

PCI DSS Section 5: Regularly Monitor & Test Networks

Requirement #10: Track & Monitor All Access To Network Resources & Cardholder Data
The City is SAQ B-IP, and this requirement does not apply.

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
The City is SAQ B-IP, and this control does not apply.

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.

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.

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

PCI DSS Control 11.4
The City is SAQ B-IP, and this control does not apply.

PCI DSS Control 11.5
The City is SAQ B-IP, and this control does not apply.

PCI DSS Control 11.6
The City is SAQ B-IP, and this control does not apply.

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.

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
The City is SAQ B-IP, and this control does not apply.

PCI DSS Control 12.3
Control Objective: The organization develops and implements usage policies for critical technologies.

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. [3]

Procedures: This is done with staff job descriptions.

PCI DSS Control 12.5
Control Objective: The organization assigns an individual or a team cybersecurity management 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.

Procedures: This is standard practice.

PCI DSS Control 12.7
The City is SAQ B-IP, and this control does not apply.

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.

[3] PCI DSS v4.0 Requirement 12.4 & 12.4.1

PCI DSS CONTROL 12.9

The City is SAQ B-IP, and this control does not apply.

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.

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

PCI DSS CONTROL 12.11

The City is SAQ B-IP, and this control does not apply.

APPENDICES

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 Retention Periods

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

Appendix C: Cybersecurity Roles & Responsibilities

C-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.

C-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.

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