City of Waukesha
PCI-DSS Policy

I. Purpose. This Payment Card Industry Data Security Standards (PCI-DSS) Policy defines the necessary measures to protect the confidentiality, integrity, and availability of City of Waukesha's payment card data and related information systems program for PCI DSS v4.0 compliance.

II. Definitions of Key Terms. Definitions of key terms used in this policy can found on the PCI Security Standards Council's website: https://www.pcisecuritystandards.org/

III. Applicability. Payment Card Industry Data Security Standard Self-Assessment Surveys (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. This policy applies to the controls required of SAQ B-IP.

IV. PCI DSS SECTION 1: BUILD & MAINTAIN A SECURE NETWORK

A. 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.

B. 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.

C. 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 practice.

D. 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.

V. PCI DSS SECTION 2: PROTECT CARD HOLDER DATA

A. 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: Encryption to the payment gateway from the card readers is handled by the payment processor.

B. 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 to thwart this. This includes SharePoint, OneDrive, Teams, and Email

VI. PCI DSS SECTION 3: MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

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.

VII. PCI DSS SECTION 4: IMPLEMENT STRONG ACCESS CONTROL MEASURES

A. 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.

B. 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.

C. PCI DSS CONTROL 8.3

Control Objective: The organization requires two-factor authentication for remote access originating from outside the Cardholder Data Environment (CDE) 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.

D. 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.

E. 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.

F. 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.

G. 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.

H. 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.

I. 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.

VIII. PCI DSS SECTION 5: REGULARLY MONITOR & TEST NETWORKS

A. 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: See the Vulnerability and Patch Management Program document for more details.

B. PCI DSS CONTROL 11.3

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

Procedures: See the Vulnerability and Patch Management Program document for more details.

IX. PCI DSS SECTION 6: MAINTAIN AN CYBERSECURITY POLICY

A. PCI DSS CONTROL 12.1

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

Procedures: This policy and the Vulnerability and Patch Management Program serve this purpose.

B. 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.

C. PCI DSS CONTROL 12.4

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

Procedures: This is done with IT staff job descriptions.

D. 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.

E. PCI DSS CONTROL 12.6

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

Procedures: This has been in place since 2017

F. PCI DSS CONTROL 12.8

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

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

G. 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: See the Cyber Incident Response Plan (IRP) for more details.

X. **Policy Updates.** This Policy will be reviewed annually by the Information Technology Board. Updates to the PCI DSS Cybersecurity Policy will be announced to employees via management updates or email announcements.

XI. **Exceptions.** A manager (or an appointed designee) seeking an exception must assess the risks that non-compliance creates for the City. 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.

XII. **Penalties for Violations.** Violations of this Policy will subject the violating employee to discipline, up to and including termination, as provided in Human Resources Policy G-3.

Approved this 18th day of June 2024

Shawn N. Reilly, Mayor

Sara Spencer, Clerk-Treasurer