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.