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