Office of the Mayor
City of Columbus
Ohio

PAYMENT CARD POLICY

Purpose and Scope
Payment (credit) card information is highly sensitive and is regulated by the Payment Card Industry Security Standards Council. Merchants who accept and process payment card information must comply with the Payment Card Industry Data Security Standard (PCI DSS) or risk fines and/or losing their right to accept credit card payments from their customers. The purpose of this *Payment Card Policy* is to ensure that City of Columbus personnel, vendors and IT systems meet the security standards detailed in the PCI DSS. The scope of this policy includes any City of Columbus official, or affiliate with responsibilities for: managing City cardholder transactions; managing IT systems that store, process or transmit cardholder data; and employees or personnel entrusted with handling or processing cardholder payments. This purpose is aligned with the Mayor's Columbus Covenant Peak Performance goals.
Applicability
This policy applies to city merchants accepting cardholder payments using a terminal as well as city merchants processing or sending transactions over the Internet. Internet transactions include links on City websites redirecting customers to another website; use of software including Point-of Sale software on a computer to transmit, process, or store credit card information; use of third party vendor to transmit, process, or store credit or debit card information; and use of cellular service. This policy requires each department that accepts cardholder payments be approved by the City Treasurer's Office and the Department of Technology and, where applicable, be approved by the City's external PCI auditor.

Table of Contents

1 Policy

It is the policy of the City of Columbus that any entity with whom the City has a relationship and may have access to cardholder data or computer systems that store, process or transmit cardholder data in which said cardholder data is related to the City acting as a merchant or acting as a service provider, shall

comply with City policy, state and federal laws, and contractual obligations to the City's banks and financial institutions, including but not limited to Payment Card Industry Data Security Standards (PCI DSS) published by the Payment Card Industry Security Standards Council and available at https://www.pcisecuritystandards.org/.

1.1 Policy Compliance

The City of Columbus is committed to safeguarding the City's information assets against unauthorized access, damage, and loss. The City of Columbus *Payment Card Policy* is a part of this protection and compliance with this policy is mandatory. Each user must understand his/her role and responsibilities regarding information security issues and protecting information. Failure to comply with this security policy that results in the compromise of information assets confidentiality, integrity, privacy, or availability may result in appropriate action as permitted by law, rule, regulation or negotiated agreement.

Penalties for PCI noncompliance are left in the hands of the acquiring banks. While the exact consequence is unknown; the acquiring bank and payment brands have the authority to do the following: levy fines; file suit; refuse the noncompliant merchant to take credit/debit cards.

1.2 Roles and Responsibilities

DEPARTMENT OF TECHNOLOGY

The Department of Technology manages IT systems on behalf of city departments. The Department of Technology must:

1) Monitor and analyze security alerts and information, and distribute to appropriate personnel;
2) Maintain and distribute an Incident Response Plan;
3) Administer user account and authentication management;
4) Control and monitor all access to electronic cardholder data.
5) Ensure that IT personnel and the systems under their management meet the security requirements set forth in the information security guidelines issued by the ISM including but not limited to all PCI DSS requirements.
6) Know and adhere to applicable information security policies, standards, guidelines and regulations.
7) Participate in information security awareness training.
8) Request access from their immediate manager.
9) Report known or suspected information security incidents or unsecure operating processes to the ISM.

CHIEF TECHNOLOGY OFFICER

The CTO oversees development, adoption and dissemination of City of Columbus information security policies, standards, and strategic direction for the City of Columbus information security program. The CTO is responsible for reviewing and approving the information security program to ensure that meets applicable Federal, State and local statutes and regulations.

The CTO will delegate to the information security manager to oversee the details and daily management of the information security program and will provide this individual with the appropriate resources and authority to carry out these tasks.

INFORMATION SECURITY MANAGER

The information security manager (ISM) is responsible for the development, implementation and maintenance of the City of Columbus information security program. The ISM has the authority to delegate specific information security tasks and responsibilities to DoT information security section personnel. The ISM will:

1) Review and update this policy at least annually and as made necessary by changes to the PCI DSS or the City's cardholder data environment and submit to the City's Best Practice Leadership for review and dissemination to the entire City.

2) Review and update an information security guideline at least annually and as made necessary by changes to the PCI DSS or the City's cardholder data environment that addresses the specific requirements of PCI DSS. The ISM will disseminate this guideline to the Department of Technology and, as necessary, to any other appropriate audience.

3) Provide assurances to the CTO and the City Treasurer that applicable City of Columbus systems are configured, administered, monitored and maintained according to current PCI DSS requirements.

4) Report known or suspected information security incidents or unsecure operating processes to the City Treasurer's Office.

CITY DEPARTMENTS INVOLVED IN ACCEPTING PAYMENT CARD INFORMATION:

City departments involved in accepting payment card information include the roles of CITY MERCHANTS, STAFF MANAGERS and STAFF. As a whole, City departments involved in accepting payment card information must:

1) Establish necessary awareness of payment card related payment process with the City Treasurer and the Department of Technology;

2) Designate a contact for PCI compliance activities;

CITY MERCHANTS/ STAFF MANAGERS

A city merchant is a person responsible for business processes, staff and systems that accept payment cards under the merchant ID governed by the City Treasurer. The city merchant may or may not directly manage staff involved in accepting payments and using systems that accept payments. In cases where the staff manager is different from the city merchant, the city merchant may delegate some of the responsibilities to the staff manager. City merchants/staff managers are responsible for:

1) Controlling and monitoring all access to any physical cardholder data.

2) Approving system access based on existing job profiles and making a request to the Department of Technology to configure system access privileges accordingly;

3) Ensuring that authorized personnel access is terminated immediately upon termination, resignation, or transfer to another position or department, including immediate notification to the Department of Technology.

4) Ensuring daily operational procedures exist for handling cardholder data, including but not limited to handling of payment cards or physically recorded data (e.g. written down), customer call ins, etc., as well as the directions for secure storage and disposal that comply with PCI DSS;

5) Ensuring that personnel under their charge adhere to all applicable information security policies, standards and regulations.

6) Ensuring that all employees that accept credit cards and those that have exposure to systems that process credit cards receive security awareness training upon hire, and annually thereafter.

7) Reporting known or suspected information security incidents or unsecure operating processes to the Department of Technology.

STAFF

Workers are broadly defined as City of Columbus employees, vendors or service providers who accept credit card payment and have been granted non-privileged access to City of Columbus information processing systems [ORC 1306.01(K)] which, in the context of this Policy, accept payment via payment card. General system users are responsible for:

1) Knowing and adhering to applicable information security policies, standards, guidelines and regulations.

2) Participating in information security awareness training.

3) Requesting access from their city merchant/staff manager.

4) Reporting known or suspected information security incidents or unsecure operating processes to their city merchant/staff manager.

EXTERNAL ENTITIES

All external entities (partnerships, contractors, vendors) who perform requisite contracted functions for the City in the handling, storage or processing of credit cards must:

1) Provide the City evidence of PCI compliance annually.

2) Immediately notify the City of any breach.

1.3 Payment Processing Standards

Below are the methods to process cardholder data identified by the PCI Council listed with the relevant Data Security Standards for each method in the Self-Assessment Questionnaires (SAQ). These are general guidelines; the external PCI auditor may require additional PCI regulations be met. Refer to the PCI Council's website for a complete listing of the standards that may apply to your processing method. https://www.pcisecuritystandards.org/

SAQ A	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. This would never apply to face-to-face merchants.	Preferred
SAQ B	Imprint-only merchants with no electronic cardholder data storage, or standalone, dial-out terminal merchants with no electronic cardholder data storage. This would never apply to e-commerce merchants.	Preferred
SAQ C-VT	Merchants using only web-based virtual terminals, no electronic cardholder data storage. This would never apply to e-commerce merchants.	
SAQ C	Merchants with payment application systems connected to the Internet, no electronic cardholder data storage.	
SAQ D	All other merchants not included in descriptions for SAQ types A through C above, and all service providers defined by a payment brand as eligible to complete an SAQ.	
SAQ P2PE-HW	Merchants using only hardware payment terminals included in a PCI SSC-listed, validated, P2PE solution, no electronic cardholder data storage. This would never apply to e-commerce merchants.	Preferred

The City prefers processing methods that minimize the scope of the cardholder data environment (CDE) by keeping all storage, processing and transmission off of the City's network. City of Columbus merchants pursuing alternatives to preferred methods must be approved by the Department of Technology, who may require approval by the City's external PCI Qualified Security Assessor (QSA) or formal certification by the PCI Security Standards Council.

1.3.1 Internet Processing

The preferred method for accepting Internet payments is for customers to be redirected to a PCI approved third party service provider to transmit, process, and/or store cardholder data.

1.3.2 Payment by Phone

The preferred method for accepting payments by phone is for customers to be redirected to a PCI approved third party service provider to transmit, process, and/or store cardholder data.

1.3.3 Card Present Processing

The preferred method for accepting face-to-face, card present payments is for customers to be presented with a customer-facing PCI approved point-of-sale device connected via analog phone line to the City's processor.

1.3.4 Emergency/Business Continuity Processing

The preferred method of processing payments in an emergency/business continuity scenario is with a cellular phone point-of-sale terminal.

1.4 Data Security Standards

The following standards reflect all requirements of the PCI DSS at a high level. City merchants must maintain procedures as required by this policy and the PCI DSS. Per Section 1.2, the ISM must maintain a detailed information security guideline that addresses the specific requirements for the management of IT systems.

At a high level, said entities involved in accepting revenue via payment cards must:

1.4.1 Build and Maintain a Secure Network

1.4.1.1 Install and maintain a firewall configuration to protect data (PCI 1)

Firewalls are devices that control computer traffic allowed into and out of the City's network, and into sensitive areas within its internal network. Firewall functionality may also appear in other system components. Routers are hardware or software that connects two or more networks. All such devices are in scope for assessment of Requirement 1 if used within the cardholder data environment.

1) The Department of Technology will establish firewall and router configuration standards that formalize testing whenever configurations change; that identify all connections to cardholder data (including wireless); that use various technical settings for each implementation; and stipulate a review of configuration rule sets at least every six months.

2) The Department of Technology will build firewall and router configurations that restrict all traffic from "untrusted" networks and hosts, except for protocols necessary for the cardholder data environment.

3) The Department of Technology will prohibit direct public access between the Internet and any system component in the cardholder data environment.

4) The Department of Technology will install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet that are used to access the organization's network.

1.4.1.2 Do not use vendor-supplied defaults for system passwords and other security parameters (PCI 2)

The easiest way for a hacker to access the City's network is to try default passwords or exploits based on default system software settings in the payment card infrastructure. Default passwords and settings for most network devices are widely known and must be changed.

1) The Department of Technology will always change vendor-supplied defaults before installing a system on the network. This includes wireless devices that are connected to the cardholder data environment or are used to transmit cardholder data.

2) The Department of Technology will develop configuration standards for all system components that address all known security vulnerabilities and are consistent with industry-accepted definitions; update system configuration standards as new vulnerability issues are identified.

3) The Department of Technology will encrypt using strong cryptography all non-console administrative access such as browser/web-based management tools.

1.4.2 Protect Cardholder Data

1.4.2.1 Protect stored cardholder data (PCI 3)

In general, no cardholder data should ever be stored unless it's necessary to meet the needs of the business. Sensitive data on the magnetic stripe or chip must never be stored. PAN data, if stored, must be rendered unreadable.

1) City merchants should not keep any cardholder data. If it is necessary, city merchants must keep cardholder data storage to a minimum by implementing data retention and disposal policies and procedures that define the legal, regulatory, and business requirements for data retention and specifically address retention requirements for cardholder data.

2) Cardholder data must be destroyed when it is no longer needed for legal, regulatory, or business reasons. Procedures must be in place that require:

    a. Physical media to be cross-cut shredded;

    b. Electronic media to be securely wiped, degaussing, or physically destroyed (i.e. grinding or shredding hard disks.);

    c. If a third party vendor is used to destroy cardholder data, the vendor must be a Level 1 service provider on the approved PCI list or be approved by NAID, National Association Information Destruction.

3) Storage of the following data elements is strictly prohibited in all circumstances:

    a. Full contents of any track or magnetic-stripe data;

    b. Three-digit or four-digit card-verification code or value printed on the front of the card or the signature panel [CVV2(Card Verification Value), CVC2(Card Validation Code), CID(Card Identification), CAV2((Card Authentication Value) data];

    c. Personal identification number (PIN) or the encrypted PIN block.

4) Terminals, computers, and receipts may display or print no more than the last four digits of the credit card number.

5) City merchants must define processes for ensuring that stored cardholder data does not exceed requirements defined in the data retention policy and perform them at least quarterly.

6) Imprint machines display the full 16 digit card number on the merchant copy and should only be used to process cardholder payments in an emergency. The merchant copy with the 16 digit card number must be securely stored.

7) City merchants must not store electronic cardholder data without the knowledge and approval of the Department of Technology.

8) The Department of Technology will protect stored cardholder data according to the requirements in the PCI guideline maintained by the ISM.

1.4.2.2 Encrypt transmission of cardholder and sensitive information across open public networks (PCI 4)

Cyber criminals may be able to intercept transmissions of cardholder data over open, public networks so it is important to prevent their ability to view these data. Encryption is a technology used to render transmitted data unreadable by any unauthorized person.

1) Use strong cryptography and security protocols [for example, SSL/TLS(Secure Sockets Layer/Transport Layer Security), IPSEC(Internet Protocol Security), SSH(Secure Shell), etc.] must be used to safeguard sensitive cardholder data during transmission over open, public networks.

2) Unprotected PANs(Primary Account Numbers) must not be sent via end-user messaging technologies. Fax, e-mail, scanned and other technologies to send cardholder data are prohibited.

1.4.3 Maintain a Vulnerability Management Program

1.4.3.1 Use and regularly update anti-virus software (PCI 5)

Many vulnerabilities and malicious viruses enter the network via users' e-mail and other online activities. Anti-virus software must be used on all systems affected by malware to protect systems from current and evolving malicious software threats.

1) The Department of Technology will deploy anti-virus software on all systems affected by malicious software (particularly personal computers and servers).

2) The Department of Technology will ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.

1.4.3.2 Develop and maintain secure systems and applications (PCI 6)

Security vulnerabilities in systems and applications may allow criminals to access PAN and other cardholder data. Many of these vulnerabilities are eliminated by installing vendor-provided security patches, which perform a quick-repair job for a specific piece of programming code. All critical systems must have the most recently released software patches to prevent exploitation. Secure coding practices for developing applications, change control procedures and other secure software development practices should always be followed.

1) The Department of Technology will ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. The Department of Technology will deploy critical patches within a month of release.

2) The Department of Technology will establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. Risk rankings will be based on industry best practices and guidelines.

3) No custom application code may be used without the approval of the Department of Technology and a PCI Qualified Security Assessor. All custom application code changes must be reviewed according to the requirements in the PCI guideline maintained by the ISM.

4) The Department of Technology will follow change control processes and procedures for all changes to system components.

5) The Department of Technology will ensure all public-facing web applications are protected against known attacks, either by performing code vulnerability reviews at least annually or by installing a web application firewall in front of public-facing web applications.

1.4.4 Implement Strong Access Control Measures

1.4.4.1 Restrict access to data by business need-to-know (PCI 7)

To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on 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.

1) Access to system components and cardholder data must be limited to only those individuals whose job requires such access and approved by authorized manager.

2) Access rights for privileged user IDs must be assigned to individuals based on job classification and function and restricted to the least privileges necessary to perform job responsibilities.

3) All access must be documented with approval and the required privileges.

4) Access controls must be implemented using an automated access control system.

1.4.4.2 Assign a unique ID to each person with computer access (PCI 8)

Assigning a unique identification (ID) to each person with access ensures that actions taken on critical data and systems are performed by, and can be traced to, known and authorized users. Requirements apply to all accounts, including point of sale accounts, with administrative capabilities and all accounts with access to stored cardholder data.

1) The Department of Technology will assign a unique ID to each person with computer access to cardholder data. User names and passwords may not be shared.

2) The Department of Technology will employ passwords to authenticate all users.

3) The Department of Technology will employ two-factor authentication for remote access to the network by employees, administrators, and third parties.

4) The Department of Technology will ensure all passwords are rendered unreadable during storage and transmission, for all system components, by using strong cryptography.

5) The Department of Technology will ensure proper user identification and authentication management for non-consumer users and administrators on all system components.

6) Upon the termination or transfer of an employee, City merchants must immediately:

    a. Revoke all physical access methods (e.g. badges, keys, etc.).

    b. Revoke all logical access for any automated access control systems managed by the merchant;

    c. Notify the Department of Technology and any third parties that manage access on behalf of the City.

7) Upon notice of the termination or transfer of an employee, the Department of Technology, and any third parties that manage access on behalf of the City, must immediately revoke all account access.

8) Department of Technology must either remove or disable inactive user accounts over ninety (90) days old.

9) Accounts used by vendors to access, support and maintain system components must be:

    a. Disabled when not being used;

    b. Enabled only when needed;

    c. Monitored while being used.

10) Group, shared, or generic accounts and passwords are prohibited.

11) Department of Technology will enforce password and account/session locking standards according to the requirements in the PCI guideline maintained by the ISM.

1.4.4.3 Restrict physical access to cardholder data (PCI 9)

Any physical access to data or systems that house cardholder data provides the opportunity for persons to access and/or remove devices, data, systems or hardcopies, and should be appropriately restricted. "Onsite personnel" are full- and part-time employees, temporary employees, contractors, and consultants who are physically present on the entity's premises. "Visitors" are vendors and guests that enter the facility for a short duration - usually up to one day. "Media" is all paper and electronic media containing cardholder data.

1) Appropriate facility entry controls must be in place to limit and monitor physical access to systems in the cardholder data environment.

2) Procedures must be in place and followed that make it easy to distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible. Employees must adhere to the *CITY-WIDE POLICY ON EMPLOYEE IDENTIFICATION BADGES.* Procedures must identify personnel who are authorized to access the badge system.

3) All visitors must be authorized before entering areas where cardholder data is processed or maintained; given a physical token that expires and that identifies visitors as not onsite personnel; and asked to surrender the physical token before leaving the facility or at the date of expiration. Not sure about the token or visitors log.

4) Visitor logs must be used to maintain a physical audit trail of visitor information and activity, including visitor name and company, and the onsite personnel authorizing physical access. The log must be retained for at least three months unless otherwise restricted by law.

5) Media back-ups must be stored in a secure location, preferably off site.

6) All media must be stored in a locked drawer or locked office or otherwise physically secured. City merchants must review the security of all cardholder data storage locations at least annually.

7) Strict control must be maintained over internal or external distribution of any kind of media. Media must be classified so the sensitivity of the data can be determined. External distribution must be transferred by secured courier or delivery method that can be accurately tracked. Internal City of Columbus mail is not an approved method of transfer.

8) Any and all media moved from a secured area must be approved by management, especially when media is distributed to individuals.

9) Strict control must be maintained over the storage, maintenance and accessibility of media. Media inventories must be conducted at least annually.

10) Media must be destroyed when it is no longer needed for business or legal reasons and must be cross-cut shredded. Electronic media must be rendered unrecoverable via secure wiping, degaussing, or physical destruction (i.e. grinding or shredding hard disks.) If a third party vendor is used to destroy cardholder data, the vendor must be a Level 1 service provider on the approved PCI list or be approved by NAID(National Association Information Destruction).

1.4.5 Regularly Monitor and Test Networks

1.4.5.1 Track and monitor all access to network resources and cardholder data (PCI 10)

Logging mechanisms and the ability to track user activities are critical for effective forensics and vulnerability management. The presence of logs in all environments allows thorough tracking and analysis if something goes wrong.

1) The Department of Technology must establish a process for linking all access to system components to each individual user – especially access done with administrative privileges.

2) The Department of Technology must implement automated audit trails for all system components for reconstructing these events: all individual user accesses to cardholder data; all actions taken by any individual with root or administrative privileges; access to all audit trails; invalid logical access attempts; use of identification and authentication mechanisms; initialization of the audit logs; and creation and deletion of system-level objects.

3) The Department of Technology must record audit trail entries for all system components for each event, including at a minimum: user identification, type of event, date and time, success or failure indication, origination of event, and identity or name of affected data, system component or resource.

4) The Department of Technology must implement time synchronization technology, synchronize all critical system clocks and times and implement controls for acquiring, distributing, and storing time.

5) The Department of Technology must secure audit trails so they cannot be altered.

6) The Department of Technology must review logs for all system components related to security functions at least daily.

7) The Department of Technology must retain audit trail history for at least one year; at least three months of history must be immediately available for analysis.

1.4.5.2 Regularly test security systems and processes (PCI 11)

Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security is maintained over time. Testing of security controls is especially important for any environmental changes such as deploying new software or changing system configurations.

1) The Department of Technology must test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis.

2) The Department of Technology must run internal and external network vulnerability scans at least quarterly and after any significant change in the network.

3) The Department of Technology must perform external and internal penetration testing, including network- and application-layer penetration tests, at least once a year and after any significant infrastructure or application upgrade or modification.

4) The Department of Technology must use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. IDS/IPS(Intrusion Detection Systems/Intrusion Prevention Systems) engines, baselines, and signatures must be kept up to date.

5) The Department of Technology must deploy file-integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files, and configure the software to perform critical file comparisons at least weekly.

1.4.6 Maintain an Information Security Policy

1.4.6.1 Maintain a policy that addresses information Security (PCI 12)

1) The ISM will review and recommend updates to this policy at least annually and as made necessary by changes to the PCI DSS or the City's cardholder data environment and submit changes to the City's Best Practice Leadership for review and dissemination to the entire City.

2) The ISM will review and update an information security guideline at least annually and as made necessary by changes to the PCI DSS or the City's cardholder data environment that addresses the specific requirements of PCI DSS. The ISM will disseminate this guideline to the Department of Technology and, as necessary, to any other appropriate audience.

3) All employees must adhere to daily operational security procedures that are consistent with requirements in PCI DSS.

1.4.6.2 Establish standards for third party service providers

Language must be included in agreements with Third Party Vendors involved in transmitting, processing, or storing credit or debit card data to comply at all times with the Payment Card Industry (PCI) Data Security Standards (DSS). Detailed information about PCI DSS can be found at the PCI DSS Council's website: www.pcisecuritystandards.org.

Third party vendors must be a certified vendor of the city's merchant card processor.

The merchant department must monitor the annual renewal date of compliance and provide to the Department of Technology.

1.4.6.3 Conduct background checks for potential employees or personnel considered for hire

Departments must perform applicable background checks, within the limits of local law and in accordance with City of Columbus Human Resources policy, on individuals considered for hire who will have access to systems, networks, or cardholder data. It is strongly recommended that any current employee or personnel who have access to more than one credit card number at a time have a background check within the limits of local law and in accordance with City of Columbus Human Resources policy. All COC employees are subject to a background check. Are we adding removal standards for certain offenses? Theft, Credit Card Fraud, etc.?

1.4.6.4 Conduct initial and annual training

Any official, administrator, or affiliate with responsibilities for managing City of Columbus cardholder transactions and employees or personnel entrusted with handling or processing cardholder payments must complete annual training, and upon hire, before processing cardholder payments.

1.4.6.5 Report security incident to appropriate authorities

If you know or suspect that cardholder data has been exposed, stolen, or misused this incident must be reported immediately to their city merchant/staff manager.

The city merchant/staff manager must report the incident to:

City of Columbus Department of Technology
Phone: 614-645-5758; Email: TechnologyServiceDesk@columbus.gov

The City of Columbus Department of Technology must report the incident to:
City of Columbus Office of the Treasurer
Phone: 614-557-2950; Email dlklie@columbus.gov

This report must not disclose by fax or e-mail cardholder data, three or four digit validation codes, or PINs(Personal Identification Numbers).

1.5 Appropriate Use

Appropriate use of technology within the cardholder data environment (CDE) is critical because of the sensitive nature of the information and the potential impact of improper use. Rules for appropriate use of the City's IT systems are defined in the *Comprehensive Electronic Communications Policy* (CECP) and apply to the CDE. This appropriate use policy restates and in some cases extends the CECP to address the requirements of the PCI DSS for applicable employees and vendors according to the scope of this policy.

All City of Columbus critical technologies, including but not limited to remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), e-mail usage and Internet usage:

1) Require explicit approval by the worker's manager prior to use;
2) Require authentication with user ID and password or other authentication as required by policy;
3) Must be accurately tracked in an inventory list;
4) Require an accurate list of personnel authorized to use the devices;
5) Require labeling to determine owner, contact information and purpose;
6) Must be approved DoT standards;
7) Must be restricted to network locations segmented from the CDE unless explicitly approved by the Department of Technology.

1.5.1 Remote-access technologies

1) Remote access to the CDE requires multi-factor authentication.
2) Remote access sessions to the CDE must automatically disconnect after 15 minutes of inactivity.
3) Remote access sessions to the CDE by vendors and business partners must be enabled only when needed and immediately deactivated after use.
4) Copying, moving, or storing of cardholder data onto local hard drives and removable electronic media when accessing such data via remote-access technologies is prohibited.

1.5.2 Wireless technologies

1) Any and all wireless networks must be segmented from the CDE.
2) Access to the CDE from wireless is considered to be remote access.

1.5.3 Removable Electronic Media

1) Copying, moving, or storing of cardholder data onto local hard drives and removable electronic media is prohibited.

1.5.4 Laptops

1) All laptops must be encrypted.

2) Use of laptops in the CDE is prohibited unless explicitly approved by the Department of Technology.

3) Copying, moving, or storing of cardholder data onto laptops is prohibited.

1.5.5 Tablets

1) Use of tablets in the CDE is prohibited unless explicitly approved by the Department of Technology.

2) Copying, moving, or storing of cardholder data onto tablets is prohibited.

1.5.6 Personal data/digital assistants (PDAs)/Smart Phones

1) Use of PDAs and/or smart phones in the CDE is prohibited unless explicitly approved by the Department of Technology.

2) Copying, moving, or storing of cardholder data onto PDAs and/or smart phones is prohibited.

1.5.7 E-mail usage

1) Cardholder data may not be faxed, e-mailed, scanned or sent by end-user messaging technologies by City of Columbus personnel. If a customer e-mails, faxes, or sends cardholder data, the following steps must be taken:

    a. Notify the customer the transaction cannot be processed; e-mail, fax, and other messaging technologies are not secure nor authorized methods to transmit cardholder data;

    b. Request the cardholder data be provided by alternate, approved method;

    c. "Shift, Delete" the e-mail or, in the case of a fax, cross-cut shred the fax immediately.

1.5.8 Internet usage

1) Internet usage from the CDE should be restricted to only what is necessary to perform job functions and not be used for personal use.

2) Internet usage from the CDE must be filtered.

2 Definitions

These definitions are a subset of those available through the PCI Security Standards Council's *Glossary of Terms, Abbreviations, and Acronyms*:

Cardholder Data	At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code
City Merchant	A city merchant is defined as any entity that accepts payment cards bearing the logos of any of the five members of PCI SSC [American Express, Discover, JCB(Japanese Credit Bureau), MasterCard or Visa] as payment for goods and/or services under the merchant ID governed by the City Treasurer.

IT Service Owners	IT Service Owners are City of Columbus managers responsible for overseeing the administration of information processing systems and data on behalf of city merchants.
PCI DSS	Payment Card Industry Data Security Standard. The PCI DSS is a result of collaboration of the PCI SSC to create common industry security requirements. Other card companies operating in the United States have also endorsed the standard within their respective programs.
PCI SSC	Payment Card Industry Security Standards Council (American Express, Discover, JCB, MasterCard or Visa).
Service Providers	Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data. This also 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. Entities such as telecommunications companies that only provide communication links without access to the application layer of the communication link are excluded.