



CITY OF DUBLIN

**CITY OF DUBLIN
ADMINISTRATIVE ORDERS
OF THE CITY MANAGER**

ADMINISTRATIVE ORDER 5.14
TO: All City Employees
FROM: Terry Foegler, City Manager <i>TJ 6/24/10</i>
SUBJECT: Payment Card Handling: PCI Compliance Policy
DATE: June 18, 2010
New Administrative Order

I. Purpose

This Administrative Order establishes the policy and procedures that the City of Dublin (the City), as a credit card merchant account holder, will use to assess and secure credit card data in paper and electronic form. It also establishes responsibility and accountability for all steps in the processing of credit card data, and adherence to the PCI Data Security Standards (PCI-DSS). The PCI-DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

This policy must be used in conjunction with the complete PCI-DSS requirements as established and revised by the PCI Security Standards Council at: <https://www.pcisecuritystandards.org/>. Without adherence to the PCI-DSS standards, the City is subject to: any fines imposed by the payment card industry; any additional monetary costs associated with remediation, assessment, forensic analysis or legal fees; and suspension of the merchant account.

II. Applicability

This policy applies to all employees who process or handle credit card data. It applies to any devices owned or leased by the City of Dublin that store, transmit, or process credit card data. It also applies to all third parties who process credit card data on behalf of a City-issued merchant account.

III. Authority

Finance is responsible for issuing credit card merchant accounts and for overseeing policies and procedures regarding payment processing. Information Technology is responsible for

the operation of applications and data networks as well as the establishment of information security policies, guidelines, and standards. These offices therefore have the authority to require that all merchant accounts and related technology adhere to the PCI-DSS requirements to protect cardholder data. Managers of affected employees will be responsible for ensuring that their personnel are aware of and adhere to this policy.

IV. Statement of Policy

The City of Dublin compliance standards are as follows:

A. General Requirements

1. The City credit card merchant accounts must be approved by Finance.
2. Any proposal for a new process or vendor relationship (electronic or paper) related to the storage, transmission or processing of credit card data must be approved by Finance and Information Technology.
3. All employees involved in processing credit card payments must have read, understood, and agree to adhere to A.O. 1.23 - Technology Use Policy, and this Administrative Order. Such employees must sign a copy of the attached "Payment Card Data Security and Software/ Facility Use Statement" certifying that they have done so, and submit the signed documentation to Finance.

B. Methods of Processing – only the following methods for processing are permitted:

1. Point of Sale Equipment (POS) approved by Information Technology and Finance.
2. Computer Applications, including Web-based processing, desktop applications or any other method approved by Finance and Information Technology.
3. Credit Card Terminal Devices (cardswipe units)
4. Use of alternative methods may be approved, on a case-by-case basis, by the Finance Department, and only after review and approval by Information Technology.

C. Specific Requirements

- 1) Neither the full contents of any track for the magnetic stripe nor the three-digit card validation code may be stored in an electronic file or database of any sort. This will be verified by Information Technology.
- 2) Displays or printouts of cardholder data may only show the last four digits of the account number.
- 3) Sensitive cardholder data, such as account numbers or expiration dates, may not be sent nor received electronically, or by email.
- 4) Access to cardholder data must be restricted to users with a need to know, as identified by the director of each work unit.

- 5) Each person with computer access to cardholder data must login with a unique user ID, either one provided by Information Technology or created for them in the application.
- 6) Physical security controls must be in place to prevent unauthorized access to cardholder data.
- 7) Third party vendors with access to cardholder data must be contractually obligated to comply with the PCI standards, and maintain compliancy in any subsequent contract extension or renewal.
- 8) Security incidents, where credit card data has been compromised or obtained by an unauthorized person, must be reported to Finance and Information Technology within one (1) hour after becoming aware of the incident. At a minimum, the following procedures will be performed:
 - a) Incident will be reported to Police.
 - b) Obtain any video surveillance, documentation, physical access logs, etc.
 - c) Determine what data was compromised.
 - d) Notify affected card holders.
- 9) Payment documentation with credit card information may not be retained in any format, paper or electronically. If for any reason, credit card data must be retained, the following conditions must be met:
 - a) Obtain prior written approval from Finance and Information Technology.
 - b) Credit Card Data must clearly be marked as confidential.
 - c) Credit Card Data must be physically secured, for example, in a locked safe with controlled access.
 - d) If Credit Card Data is requested by an appropriate third party, it must be securely transmitted via courier service including the use of a tracking mechanism.
 - e) Credit Card Data needs to be securely destroyed immediately after it is no longer needed, so that it cannot be reconstructed.



CITY OF DUBLIN.

**City of Dublin
Payment Card Data Security and
Software/Facility Use Statement**

As a member of the staff of the City of Dublin, I may be provided with access to personal, proprietary, and/or otherwise confidential data. This can include credit card data and other confidential data from staff, patrons or other person's for which the City provides service.

As an individual whose position requires interaction with credit cards and credit card data, I may be provided with direct access to confidential and valuable data in paper and electronic form. In the interest of maintaining the integrity of these systems and processes and to ensure the security and proper use of City resources, I will:

- Maintain the confidentiality of my password for all systems to which I have access.
- Maintain in strictest confidence the credit card data to which I have access. Any confidential information must not be shared in any manner with others who are unauthorized to view such data.
- Use my access to the City's systems for the sole purpose of transaction processing related to the official business of the City. Understand that the use of these systems and their data for personal purposes is prohibited.
- Ensure that such data is shredded or otherwise disposed of in a secure and complete fashion.
- Understand that any abuse of access to the City's systems and their data, any illegal use or copying of software or any misuse of the City's equipment may result in disciplinary action and loss of access to the City's systems.

I understand that I am bound by all applicable City policies. I have read and understand such policies and agree to be held accountable and hold others accountable for their implementation.

Name _____ Date _____

Signature _____