

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

SUBJECT	Number 95.51	Issue 1	Page 1 of 9
PAYMENT CARD INDUSTRY (PCI) COMPLIANCE POLICY	Effective Date May 22, 2015		

1. PURPOSE

- 1.1. To establish a policy that outlines the requirements for compliance to the *Payment Card Industry Data Security Standards (PCI-DSS)*. Compliance with this standard is a condition of the City's acceptance of *Payment Cards* from citizens and businesses in exchange for the provision of City Services.
- 1.2. To establish a policy that is designated to protect cardholder information of patrons that utilize a *Payment Card* to transact business with the City of San Diego.
- 1.3. This policy is intended to be used in conjunction with the complete *PCI-DSS* requirements as established and revised by the *PCI Security Standards Council*.

2. SCOPE

- 2.1. This Administrative Regulation (A.R.) applies to all City employees, contractors, vendors, and other individuals that accept or have access to *Payment Card* transactions under the City's control.
- 2.2. This policy and procedures apply to all credit card data created, owned, stored, managed or under the control of the City of San Diego, regardless of the media which contains the information, including but not limited to paper, microfilm, microfiche or any analog or digital format.

3. DEFINITIONS

- 3.1. City's IT Service Provider(s) – Responsible for providing, operating and maintaining the City's primary computer systems, email systems, network services and internet connectivity, and business applications.
- 3.2. Information Technology Business Leadership Group (ITBLG) – Comprised of Director level representatives that review, prioritize and approve all IT investment proposals.
- 3.3. Merchant Account – A type of bank account that accepts payments by *Payment Cards*. A *merchant account* is coordinated through and established by the Office of the City Treasurer in consultation with the City's bank.

(New Administrative Regulation 95.51, Issue 1, effective May 22, 2015)

Authorized

[Signature on File]
CHIEF OPERATING OFFICER

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

SUBJECT	Number 95.51	Issue 1	Page 2 of 9
PAYMENT CARD INDUSTRY (PCI) COMPLIANCE POLICY	Effective Date May 22, 2015		

- 3.4. Payment Card – A debit or credit card that is accepted as payment for goods, services, or other obligations owed.
- 3.5. Payment Card Data – Full magnetic strip or the PAN, including any of the following: (1) Cardholder Name, (2) Expiration Date, and (3) Service Code.
- 3.6. Payment Card Industry (PCI) Compliance – Adherence to a set of security and reporting standards developed to protect cardholder information during and after the processing of a payment card transaction.
- 3.7. Payment Card Industry Data Security Standard (PCI-DSS) – Payment Card Industry Data Security Standard. A set of twelve (12) broad security requirements established by the PCI Security Standards Council. City Departments that accept Payment Card transactions are required to meet these standards or risk losing the capability to accept Payment Cards for services. The requirements are listed in the following table:

Control Objectives	PCI-DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a <u>firewall</u> configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system <u>passwords</u> and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data
	4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or <u>programs</u>
	6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know
	8. Identify and authenticate access to system components
	9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

SUBJECT	Number 95.51	Issue 1	Page 3 of 9
PAYMENT CARD INDUSTRY (PCI) COMPLIANCE POLICY	Effective Date May 22, 2015		

- 3.8. Payment Card Industry Security Standard Council - A consortium of major *Payment Card* providers that have established data security standards for merchants. The *PCI Security Standards Council* defines credentials and qualifications for assessors and vendors.
- a. The PCI requirements set by the *PCI Security Standards Council* do not allow for exceptions. If you have any questions about *PCI Compliance Implementation*, please forward your inquiry to COSD-PCI@sandiego.gov .
- 3.9. Primary Account Number (PAN) – The *Payment Card* number (credit or debit) that identifies the issuer and individual cardholder account. It is also called Account Number.
- 3.10. Self-Assessment Questionnaire (SAQ) – The PCI Self-Assessment Questionnaire is a validation tool primarily used by merchants to demonstrate compliance with the *PCI-DSS*.
- 3.11. Service Provider – A *PCI compliant* third party directly involved in the storage, processing or transmission of cardholder data on behalf of the City.

4. POLICY

4.1. General Policy

- 4.1.1. The City will use *PCI compliant* third party vendors to encrypt and store *Payment Card Data*.
- 4.1.2. Departments are prohibited from storing any *Payment Card Data* in an electronic format on any City computer, server, or database and further are prohibited from emailing *Payment Card Data*. In addition, any *Payment Card Data* that is written down must be either shredded or placed in a securely locked storage device immediately following the completion of the transaction.
- 4.1.3. The *City's IT Service Providers* working with the City to process *Payment Card Data* are subject to A.R. 90.63 – Information Security Policy and A.R. 90.64 – Protection of Sensitive Information and Data.
- 4.1.4. Contractors and vendors processing *Payment Card* transactions on behalf of the City are required to be *PCI compliant* at all times. In addition, contractors and vendors must provide certification annually of their continued compliance with *PCI-DSS*.
- 4.1.5. Departments must obtain authorization to process *Payment Card* transactions from the Office of the City Treasurer and Department of Information Technology. This review process will ensure that *Payment Card* processing is in compliance with this policy.

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

SUBJECT	Number 95.51	Issue 1	Page 4 of 9
PAYMENT CARD INDUSTRY (PCI) COMPLIANCE POLICY	Effective Date May 22, 2015		

4.2. Departmental Policy

- 4.2.1. Department Directors are responsible for compliance with the provisions of this A.R.
- 4.2.2. Departments must receive approval from the City’s *ITBLG* Committee prior to the start of any project and/or solicitation related to *Payment Card* transactions.
- 4.2.3. Departments will be responsible for completing the annual required SAQ and submitting it to the Office of the City Treasurer. Any remediation actions identified from this assessment or by the Department of Information Technology must be implemented immediately by the Department to ensure continue compliance.
- 4.2.4. Departments are responsible for ensuring that employees who process *Payment Card* transactions receive annual *PCI_DSS* compliance training coordinated by the Department of Information Technology. The level and content of training must be appropriate to the job functions of the employee.
 - a. Existing employees that are not current with this training should not be allowed to process *Payment Card* transactions.
 - b. New employees must receive the City approved *PCI Compliance* training prior to processing any *Payment Card* transactions .
- 4.2.5. Departments must provide employees access to equipment and systems for processing *Payment card* transactions based on a functional role (job duties) and not linked directly to the individual employee.
 - a. When an authorized employee’s job duties no longer require access to equipment or systems that process *Payment Card* transactions, access must be removed.
- 4.2.6. Appointing Authorities or their designee must, at a minimum, annually review their list of employees, contractors or other individuals that process *Payment Card* transactions to ensure continued authorization is warranted and to update (add, delete or modify) the authorization list.

4.3. User Policy

- 4.3.1. Employees who process *Payment Card* transactions are subject to A.R. 90.64 – Protection of Sensitive Information and Data.

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

SUBJECT	Number 95.51	Issue 1	Page 5 of 9
PAYMENT CARD INDUSTRY (PCI) COMPLIANCE POLICY	Effective Date May 22, 2015		

- 4.3.2. Employees must utilize *Payment Card* equipment, systems and information only for its intended purpose.
- 4.3.3. An employee or individual authorized to process *Payment Card* transactions must complete Attachment 1 – *Payment Card Industry (PCI) Compliance Authorization Acknowledgement Form*.
- 4.3.4. Violation of this A.R. either by unauthorized or authorized persons accessing or using *Payment Card Data* for reasons other than its intended purpose or beyond the scope of duties, may result in disciplinary action, up to and including termination of employment and may subject the violator to personal liability.
 - a. In the case of contractors or vendors, violation of this A.R. will be considered a breach of contract and may be referred to the appropriate agency for civil and/or criminal action, as applicable.

5. RESPONSIBILITY

5.1. Department of Information Technology

- 5.1.1. Oversee enforcement of this A.R. and investigate any reported violations of the A.R.
- 5.1.2. Lead investigations pertaining to *Payment Card* security breaches.
- 5.1.3. Terminate access to protected information if employee fails to comply with the A.R.
- 5.1.4. Work in conjunction with the Office of the City Attorney and the Purchasing and Contracting Department to create and maintain standard contract language specific to *PCI Compliance* and requirements. Review the contract language annually to ensure it remains current.
- 5.1.5. Maintain daily operational security procedures consistent with the latest *PCI-DSS* standards, including administrative and technical procedures for each of the requirements.
- 5.1.6. Maintain daily administrative and technical operational security procedures consistent with the *PCI-DSS* (e.g. user account maintenance and log review procedures).
- 5.1.7. Provide results of all required Network Scans with the appropriate remediation steps for any identified abnormal results to the *ITBLG Committee* and the Office of the City Treasurer.

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

SUBJECT	Number	Issue	Page
	95.51	1	6 of 9
PAYMENT CARD INDUSTRY (PCI) COMPLIANCE POLICY	Effective Date May 22, 2015		

- 5.1.8. Coordinate an annual review of the policy with the Office of the City Treasurer.
- 5.1.9. Work with Departments in conjunction with the Office of the City Treasurer to provide annual *PCI Compliance* training to employees and the City's IT Service Providers.
- 5.1.10. Distribute citywide *PCI Compliance* training report annually, listing all employees required to attend training and training status. The citywide *PCI Compliance* training report will be distributed to each Department Director, Chief Financial Officer, Deputy Chief Operating Officers and the Assistant Chief Operating Officer.

- 5.2. Office of the City Treasurer
 - 5.2.1. Keep a current list of Service Providers utilized by the City for *Payment Card* processing.
 - 5.2.2. Conduct annual *PCI Compliance* verification with Service Providers and report findings to *ITBLG*.
 - 5.2.3. Track any non-compliant vendors and their remediation efforts and work with departments to replace vendors who do not become compliant within the City's required timeframe, as coordinated by the Office of the City Treasurer and Department of Information Technology.
 - 5.2.4. Coordinate and consolidate all City department annual SAQ responses.
 - 5.2.5. Serve as the primary contact for Departments with business operations questions about this A.R.

- 5.3. Purchasing and Contracting
 - 5.3.1. Ensure that all solicitations involving services or hardware to process *Payment Card* transactions have been approved through the *ITBLG* process.
 - 5.3.2. Ensure solicitations, related to *Payment Card* transaction services and/or hardware/software, include the requirement for a vendor to be *PCI Compliant* and maintain *PCI Compliance*.
 - 5.3.3. Verify that all accepted vendor proposals have documentation acknowledging that the proposed service or hardware/software is *PCI Compliant* and confirm the validity of the documentation.

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

SUBJECT	Number 95.51	Issue 1	Page 7 of 9
PAYMENT CARD INDUSTRY (PCI) COMPLIANCE POLICY	Effective Date May 22, 2015		

5.3.4. Ensure that standard *PCI Compliance* language referenced in 5.1.4 is included as an Addendum, as applicable, to or within the Terms and Conditions of signed contracts and agreements for vendors and contractors who provide any *Payment Card* related services for the City of San Diego.

APPENDIX

Legal References

PCI-DSS v3.0 requirements

Administrative Regulation 90.62 – Information & Communications Technology Acceptable Use

Administrative Regulation 90.63 – Information Security Policy

Administrative Regulation 90.64 – Protection of Sensitive Information and Data

Administrative Regulation 95.10 – Identification of City Employees and Controlled Access to City Facilities

Administrative Regulation 95.20 – Public Records Act Requests and Civil Subpoenas; Procedures for Furnishing Documents and Recovering Costs

Administrative Regulation 95.50 – Credit Card Acceptance and Processing

Administrative Regulation 95.60 – Conflict of Interest and Employee Conduct

Civil Service Rule – Definition of Appointing Authority (p.1)

Civil Service Rule XI – Resignation, Removal, Suspension, Reduction in Compensation, Demotion

Personnel Manual, Index Code A-3 – Improper Use of City Resources

Personnel Manual, Index Code G-1 – Code of Ethics and Conduct

IT Security Guidelines and Standards

Employee Performance Plans, Ethics and Integrity Section

Applicable California State Laws

Applicable Federal Laws

Forms

Attachment 1 – Payment Card Industry (PCI) Compliance Authorization Acknowledgement Form

Subject Index

PCI Compliance

Payment Card

Administering Departments

Department of Information Technology

Office of the City Treasurer

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

SUBJECT	Number 95.51	Issue 1	Page 8 of 9
PAYMENT CARD INDUSTRY (PCI) COMPLIANCE POLICY	Effective Date May 22, 2015		

ATTACHMENT 1

**City of San Diego
Payment Card Industry (PCI) Compliance
Authorization Acknowledgement Form**

Authorized Person

Name (Printed)	Job Classification	Network (AD) Login/User ID
Department/Division		
Mail Station	Office Phone	
Supervisor's Name (Printed)	Supervisor's Title	Supervisor's Phone

Policy Summary (pertinent excerpts from Administrative Regulation):

- 4.3.1 Employees who process Payment Card transactions shall be subject to A.R. 90.64 - Protection of Sensitive Information and Data.
- 4.3.2 Employees must utilize Payment Card equipment, systems and Information only for its intended purpose.
- 4.3.3 An employee or individual authorized to process Payment Card transactions must sign an Authorization Acknowledgement Form attesting to have read, understood, and agreed to abide by this policy.
- 4.3.4 *Violation of this policy, either by unauthorized or authorized persons accessing or using Payment Card data for reasons other than its intended purpose or beyond the scope of duties, may result in disciplinary action, up to and including termination of employment and may subject the violator to personal liability. (a) In the case of contractors or vendors, violation of this policy will be considered a breach of contract and may be referred to the appropriate agency for civil and/or criminal action, as applicable.*

CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

SUBJECT PAYMENT CARD INDUSTRY (PCI) COMPLIANCE POLICY	Number 95.51	Issue 1	Page 9 of 9
	Effective Date May 22, 2015		

Acknowledgement

By signing below, the above employee acknowledges that he or she has been provided a full copy of the A.R. 95.51 - Payment Card Industry (PCI) Compliance Policy, which has been discussed with his or her supervisor, and further acknowledges having read, understood, and agrees to comply with the provisions of the policy. The employee understands that this form will be kept as part of his or her permanent employee file and that he or she may receive a copy, if requested. The supervisor acknowledges having discussed the policy with the above employee and understands the supervisor's obligations regarding the employee's access to Payment Card Data under this policy.

Employee's Signature

Date Signed

Supervisor's Signature

Date Signed