CITY OF SAN DIEGO
ADMINISTRATIVE REGULATION

| SUBJECT | Number | Issue | Page |
|---|---|---|---|
| | 95.51 | 2 | 1 of 8 |
| PAYMENT CARD INDUSTRY (PCI) COMPLIANCE | Effective Date<br>July 2, 2026 | | |

1. PURPOSE

1.1. To establish an Administrative Regulation (A.R.) that outlines the requirements for compliance with the *Payment Card Industry Data Security Standards* (*PCI-DSS*). Compliance with this standard is a condition of the City of San Diego's (City) acceptance of *Payment Cards* from citizens and businesses in exchange for the provision of City services.

1.2. To establish an A.R. that is designated to protect cardholder information of patrons that utilize a *Payment Card* to transact business with the City.

1.3. This A.R. 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 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 A.R. 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 paper, microfilm, microfiche or any analog or digital format.

3. DEFINITIONS

3.1. *Cardholder Data Environment* – The system components, people, and processes that store, process, or transmit cardholder data or sensitive authentication data, and system components that may not store, process, or transmit cardholder data or sensitive authentication data but have unrestricted connectivity to system components that store, process, or transmit cardholder data or sensitive authentication data.

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

Authorized

[Signature on File]

MAYOR TODD GLORIA

3.2. *City's Information Technology (IT) Service Provider(s)* – Responsible for providing, operating and maintaining the City's primary computer systems, email systems, network services, internet connectivity and business applications.

3.3. *IT Governance* – The process by which Information Technology managers gather to review a given IT solution's compliance with all applicable IT policies, standards, and guidelines.

3.4. *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.

3.5. *Payment Card* – A debit or credit card that is accepted as payment for goods, services, or other obligations owed.

3.6. *Payment Card Data* – Full magnetic strip or the *PAN*, including any of the following: (1) cardholder name, (2) expiration date, and (3) service code.

3.7. *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.

3.8. *Payment Card Industry Data Security Standard (PCI-DSS)* – A set of twelve 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. A full list of the security requirements can be located on the PCI Security Standards Council's website https://www.pcisecuritystandards.org/

3.9. *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.

3.9.1. 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 PCI@sandiego.gov.

3.10. *Point of Sale (POS)* –An electronic payment system which captures and transmits the customer's credit or debit card number and sale information to the merchant's financial institution for approval and payment.

3.11. *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.

3.12. *Qualified Security Assessor (QSA)* – An independent security organization that have been qualified by the *PCI Security Standards Council* to validate an entity's adherence to *PCI-DSS*.

3.13. *Self-Assessment Questionnaire (SAQ)* – The PCI Self-Assessment Questionnaire is a validation tool primarily used by merchants to demonstrate compliance with the *PCI-DSS.*

3.14. *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, transmit, 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, Departments are prohibited from writing down any *Payment Card Data* or storing it in any physical storage location. If any documents containing unredacted *Payment Card Data* are discovered in any physical or electronic City record, the data must be redacted or the full record deleted if it has been retained beyond the required length of time as outlined by the City's record retention schedule.

4.1.3. All City operations pertaining to credit card acceptance and processing must comply with all requirements listed in the Information Security PCI Policy, Standards, and Guidelines, which the Department of Information Technology annually reviews and updates.

4.1.4. Employees who accept and process Payment Card Data are subject to A.R. 90.50 – Credit Card Acceptance and Processing.

4.1.5. 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.

4.1.6. 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*.

4.1.7. 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 A.R.

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 via the Department of Information Technology's *IT Governance* process prior to the start of any project or solicitation related to *Payment Card* transactions.

4.2.3. Departments that wish to begin using any new credit card payment options, including the use of pre-approved *POS* terminals by the Office of the City Treasurer's contracted merchant processor, must abide by all policies and procedures identified in A.R. 95.50.

4.2.4. The Department of Information Technology 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 must be implemented immediately by the City to ensure continued compliance.

4.2.5. The Department of Information Technology will be responsible for contracting with a *QSA* to collaboratively develop, review, and approve an annual *SAQ* and attestation of compliance.

4.2.6. Departments are responsible for ensuring that employees who process *Payment Card* transactions receive the necessary training to operate relevant *POS* terminals and any connected accessories. The level and content of training must be appropriate to the job functions of the employee.

4.2.7. 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.

4.3. User Policy

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

4.3.2. Employees must use *Payment Card* equipment, systems and information only for its intended purpose.

4.3.3. 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 or criminal action, as appropriate.

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. Maintain list of *City IT Service Provider* staff who have been granted any level of access to the City's *Cardholder Data Environment*.

5.1.3. Lead investigations pertaining to *Payment Card* security breaches.

5.1.4. Terminate access to protected information if an employee fails to comply with the A.R.

5.1.5. 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.

5.1.6. Maintain daily operational security procedures within the Information Security PCI Policy, Standards, and Guidelines consistent with the latest *PCI-DSS* standards, including administrative and technical procedures for each of the requirements.

5.1.7. Maintain daily administrative and technical operational security procedures consistent with the *PCI-DSS* (e.g. user account maintenance and log review procedures).

5.1.8. Coordinate an annual review of the policy with the Office of the City Treasurer.

5.1.9. Provide annual *PCI Compliance* training to employees designated as device inspectors for *POS* terminals issued by the City's bank merchant processor. The Department of Information Technology can designate local device inspectors within customer Departments for informal inspections but can also choose to directly conduct and document formal inspections when deemed necessary.

5.1.9.1. Departments are required to designate an inspector.

5.1.9.2. Informal and formal inspections follow the same process, with informal inspections being conducted within the normal course of business when interacting with *POS* terminals while formal inspections are conducted according to a pre-defined schedule and documented/logged within a document retention site hosted by the Department of Information Technology.

5.1.9.3. If terminals are issued by a third-party *Service Provider*, a designated staff member within the Department shall provide custom inspection training to all relevant staff tasked with performing informal and formal inspections. Inspections may also be conducted directly by third party *Service Providers* if formalized in a contractual agreement.

5.1.10. Maintain a list of *Service Providers* used by the City for *Payment Card* processing.

5.1.11. Conduct annual *PCI Compliance* verification with *Service Providers* and report findings to the City's *QSA*.

5.1.12. 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.

5.1.13. Coordinate and consolidate all City department annual *SAQ* responses.

5.1.14. Serve as the primary contact for Departments with business operations questions about this A.R.

5.2. Office of the City Treasurer

5.2.1. Serve as primary contact to the City's bank merchant processor.

5.2.2. Maintain an inventory of the City's bank merchant processor-issued *POS* terminals.

5.2.3. Coordinate the delivery and replacement of all bank merchant processor-issued *POS* terminals for all City Departments.

5.2.4. Deliver the City's annual *QSA*-certified *SAQ* and any other PCI-relevant documentation to the City's bank merchant processor.

5.2.5. Inform the City's bank merchant processor of any potential discovery of fraud or data breaches.

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 *IT Governance* process.

5.3.2. Ensure solicitations, related to *Payment Card* transaction services 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.

5.3.4. Ensure that standard *PCI Compliance* language referenced in 5.1.5 is included as an Addendum, or within the contracts and agreements for vendors and contractors who provide any *Payment Card* related services for the City.

| SUBJECT | Number | Issue | Page |
|---|---|---|---|
| | 95.51 | 2 | 8 of 8 |
| PAYMENT CARD INDUSTRY (PCI) COMPLIANCE | Effective Date<br>July 2, 2026 | | |

# APPENDIX

Legal References
PCI-DSS 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
Information Security PCI Standards and Guidelines
Employee Performance Plans, Ethics and Integrity Section
Applicable California State Laws
Applicable Federal Laws

Subject Index

PCI Compliance
Payment Card

Administering Departments

Department of Information Technology
Office of the City Treasurer