LOS ANGELES UNIFIED SCHOOL DISTRICT
POLICY BULLETIN

TITLE: Payment Card Industry (PCI) Compliance

NUMBER: BUL-131110

ISSUER: David D. Hart, Chief Business Officer
Office of the Chief Business Officer

Joy Mayor, Controller
Accounting and Disbursements Division

DATE: December 19, 2022

ROUTING
Region
Administrators of Operations
Community of School Administrators
Principals
School Administrative Assistants
Office Managers
Financial Managers

POLICY: Los Angeles Unified School District (LAUSD) departments and school administrative offices that are accepting electronic payment via credit and/ or debit cards must be compliant with the requirements outlined by the by the Payment Card Industry Data Security Standards (PCI-DSS).

MAJOR CHANGES: This is a new policy in connection with the LAUSD's handling of electronic payment cards. This is to provide LAUSD with clear and manageable steps to protect customer Cardholder Data and to protect the District and its families, students, vendors, and other community members from a cardholder breach by complying with PCI-DSS.

GUIDELINES:

I. OVERVIEW

In 2006, PCI-DSS developed a set of operating and technical compliance requirements to address the security concerns resulting from the widespread use of payment cards. The major credit card companies (American Express, Discover Financial Services, JCB, Visa International, and MasterCard Worldwide) were instrumental in forming the Payment Card Industry Security Standards Council (PCI-SSC) with an expectation that entities that utilize payment cards would adhere to the guidelines and requirements outlined by the PCI-SSC.

Today, organizations like LAUSD that accept payments via payment cards must comply with these standards regardless of the size of the institution and/or the number of payment card transactions handled. The goal of the PCI-DSS is to help protect Cardholder Data (see Attachment A for definition of Cardholder Data).

This document sets forth LAUSD's policy for complying with the PCI-DSS. At a high level, the PCI-DSS is comprised of six categories and twelve requirements.

PCI-DSS requirements (see Attachment C) are dependent on an organization's merchant level (see Attachment B). PCI-DSS compliance is a continuous process. LAUSD will be monitored by its compliance with each of the requirements. LAUSD shall assess, remediate, and report its compliance status on an on-going basis. While the law does not mandate PCI-DSS compliance, non-adherence to PCI-DSS can subject LAUSD to significant financial and reputational risks. Failure to comply can result in:

a) fines and penalties imposed by payment card institutions and banks;

b) monetary costs associated with legal proceedings, settlements, and judgements; and

c) suspension of the merchant account and the inability to accept payment cards for payment.

II. SCOPE, ROLES AND RESPONSIBILITIES

This Policy applies to LAUSD personnel at schools and departments that have access to Cardholder Data and to the people, processes and technology that handle Cardholder Data at or on behalf of LAUSD. This includes, but is not limited to, any LAUSD school, department, office, employee (full-time, part-time and temporary), volunteer, student, vendor, software, computer, and/or electronic devices, involved in processing Cardholder Data on behalf of LAUSD.

LAUSD is committed to safeguarding personal information conveyed in processing debit and credit card payments and strives to be PCI-DSS compliant by using secure methods to process payment card transactions to serve its students, parents, and community members. The Division of Accounting and Disbursement is responsible for coordinating LAUSD's response to PCI compliance and works with point persons across all areas of the LAUSD to address PCI related tasks and activities.

III. GENERAL REQUIREMENTS, POLICIES AND PROCEDURES

In handling Personally Identifiable Information, the following policies and procedures must be followed.

A. Storage of Sensitive Authentication Data and Cardholder Data

a. Storage of electronic and/or physical Cardholder Data or Sensitive Authentication Data poses significant risks and increases the number of requirements that must be satisfied to be PCI-DSS compliant. PCI-DSS prohibits the storage of Sensitive Authentication Data, even if the data is encrypted. Sensitive Authentication Data includes the full contents of any data on a card's magnetic stripe, card verification codes or values (CVC/CVV) and personal identification numbers (PIN).

b. Electronic and physical Cardholder Data shall not be stored unless there is a justified business need to do so. LAUSD and Related Entities wishing to store Cardholder Data, specifically full Primary Account Numbers (PANs), shall define and document the business need for storage, including maintaining a list of all roles that require access to full PANs and staff who have such roles. Documentation must be kept up to-date and readily available in the event of an audit.

c. Notwithstanding the foregoing, the following Cardholder Data may be retained after a transaction is successfully processed for the retention period described in this Policy: payment cardholder name, transaction authorization number, transaction date, and transaction dollar amount.

B. Access to Cardholder Data

a. Cardholder Data is classified as confidential data under the LAUSD Data Classification Standard.

b. Access to Cardholder Data shall be restricted to those individuals whose job responsibilities require such access, on a strict need to know basis. This includes fulltime, part-time, temporary, contracted resources, or Related Entity employees.

c. Offices and departments that handle Cardholder Data shall define and document the roles and responsibilities of those individuals whose job functions require them to access Cardholder Data.

d. Cardholder Data-handling job functions must be instructed to not disclose any Cardholder Data, unless deemed necessary by a supervisor in accordance with PCI-DSS requirements and LAUSD policies.

C. Protecting Stored Cardholder Data

a. Departments, schools, and Related Entities with a justified business need to store Cardholder Data must ensure that Cardholder Data is appropriately protected. If there is a justified business need, the cardholder's name, PAN, expiration date, and service code may be stored if protected in accordance with PCI-DSS requirements.

b. The PAN must be masked anywhere it is displayed, such as on receipts, so that only the first six and/or the last four digits are displayed as one method of protecting stored Cardholder Data. Other methods include encryption or truncation.

D. Retention of Cardholder Data

a. Any Cardholder Data that must be retained after transaction authorization on the basis of a documented and justified business need must be kept secured and only accessible by those whose job requires that they have access to the data.

b. Physical media containing Cardholder Data must be stored in a filing cabinet or safe that is locked at all times (during and after business hours).

c. Card Verification Codes or Values (CVC/CVV) and Personal Identification Numbers (PINs) must never be retained.

d. Cardholder Data shall not be retained for more than one year.

e. Departments, schools and Related Entities shall determine a quarterly process for identifying and securely deleting or destroying stored Cardholder Data at the end of its retention period.

E. Disposal of Cardholder Data

a. Except for Cardholder Data being retained based on a justified business need, any Cardholder Data captured to process a transaction shall be purged, deleted, or destroyed, in an irretrievable manner, immediately after authorization. The following are approved techniques for disposing of Cardholder Data:

   i. Paper shall be shredded, using a crosscut shredder, pulped, or incinerated.

   ii. Digital storage media, such as CDs, DVDs, Disks, USB Drives, etc. must be securely overwritten or physically destroyed in a manner that prevents unauthorized disclosure, as per PCI-DSS requirements.

b. Cardholder Data awaiting disposal must be stored in a secure container with a lock to prevent access. The container must be labeled "classified" or have a similar label to indicate the sensitivity of the data.

F. Receipt of Cardholder Data via End-User Messaging Technologies and other methods

a. Departments, schools, and Related Entities shall not accept Cardholder Data via end-user messaging technologies (i.e., email, instant message, text message, etc.), which are not a secure means of transmission.

b. If an office or department receives Cardholder Data via end-user messaging, the message shall be deleted. The office or department shall compose a new email or text message to the sender advising them to refrain from sending Cardholder Data through this means of communication and provide proper credit card submission instructions.

c. Cardholder Data received through end-user messaging shall not be processed.

d. All forms and other documents that collect Cardholder Data shall exclude email and/or cell phone number fields as a method of submission.

e. Cardholder Data may be accepted by fax if the machine does not store the data in memory, converts the fax into email, or is not connected to the local network (i.e., a dedicated fax machine).

G. Self-Assessment Questionnaire (SAQ)

a. The Office of Accounting and Disbursement will be responsible for the completion of an annual Self-Assessment Questionnaire that will cover each department, school and Related Entity or office that processes payment card transactions using the LAUSD enterprise solution and approved equipment.

b. Departments, schools and Related Entities that are using solutions outside of LAUSD approved solutions and equipment shall complete an SAQ (see Attachment D) annually to demonstrate its compliance with PCI-DSS.

H. Internal and External Vulnerability Scans

a. Each department, school, and Related Entity must ensure that it does not store, process, or transmit Cardholder Data on or through the LAUSD network.

b. If a department, school, or Related Entity is found utilizing solutions or equipment that reside on the LAUSD network, it must conduct vulnerability scans, at least on a annual basis and after any significant changes, as required by the PCI-DSS. A PCI-validated Approved Scanning Vendor must conduct external vulnerability scans. For additional information, refer to Internal and External Vulnerability Scanning Procedures.

I. Third-Party Vendor and Service Provider Compliance

a. Third-party vendors and/or service providers that store, process, or transmit Cardholder Data on behalf of a department, school or Related Entity can impact the security of LAUSD and must be PCI-DSS compliant.

b. LAUSD has an established process for engaging third-party vendors and/or service providers, including confirming the third-party's PCI compliance status by checking the appropriate database (i.e., the VISA Global Registry).

c. LAUSD shall maintain an up-to-date list of all vendors and/or service providers, including a description of the services provided and the type of data shared with the third-party.

d. Due to evolving PCI standards, LAUSD shall verify the PCI compliance status of third parties by requesting and reviewing an Attestation of Compliance (AOC), annually.

J. Access to System Components containing Cardholder Data

a. If departments, schools or Related Entities utilize a system component handling Cardholder Data (i.e. Virtual Terminal or payment processing platform), they shall assign a unique ID or username to each person with access and add and remove a person's access as needed and as soon as the person's access authority has changed.

b. Access for users who separate from the department, school, or Related Entity or whose job responsibilities no longer require such access shall be immediately revoked and removed.

c. Departments, schools and Related Entities shall ensure that all users secure their accounts with strong passwords, that are changed at least every 90 days. As per PCI-DSS requirements, passwords must, at least, meet the following parameters:

i. A minimum password length of at least seven characters

ii. Contain both numeric and alphabetic characters

d. Departments, schools and Related Entities shall not use generic or shared user IDs and passwords and shall remove all generic user IDs prior to the utilization of the system component.

K. Point-of-Sale (POS) Devices and Protection against Skimming and Tampering

a. Point-of-Sale (POS) devices that are purchased or owned by a department, school or Related Entity as part of LAUSD's program are in-scope for PCI compliance. POS devices obtained outside of LAUSD's approved program are subject to the same requirements, but the individual department, school or Related Entity is individually responsible for ensuring the integrity of their equipment and PCI compliance.

b. PCI-DSS requirements call for the protection from tampering and skimming of devices that capture payment card data via direct physical interaction and all devices shall be physically inspected on a quarterly basis.

c. All inspections shall be documented in a log that includes the date/time and person conducting the examination. The inspections shall cover all devices recorded in LAUSD's up-to-date device inventory log, which includes the device name, model, serial #, and location of device.

L. Disposition of Point-of-Sale (POS) Devices

a. LAUSD shall disconnect Point-of-Sale devices or terminals that have been inactive for two years.

b. Departments, schools, and Related Entities with disconnected devices shall return the devices to LAUSD's Accounting and Disbursement Division for proper handling.

M. Protection of Networks and Systems

a. Departments, schools, and Related Entities shall establish and implement methods for protecting networks and systems that process, store, or transmit Cardholder Data, including but not limited to testing all network connections and changes to firewall configurations, maintaining network diagrams, using strong cryptography, maintaining up-to-date and actively running anti-virus programs and updating security patches in a timely manner, as required by PCI-DSS.

b. LAUSD will make all efforts to limit and reduce the scope of required compliance with PCI-DSS by isolating and segmenting areas of the network and systems used to process Cardholder Data, ultimately striving to keep Cardholder Data isolated from the general LAUSD network.

N. Annual PCI Awareness Training

   a. All departments, schools, and Related Entity staff with access to Cardholder Data shall take the PCI Awareness course, offered on LAUSD's Learning Network, before gaining access to Cardholder Data and at least annually thereafter.

O. Fraud Reporting Procedures

   a. Departments, schools, and Related Entities shall follow LAUSD's breach reporting procedures in the event of any alleged fraudulent or criminal activity or breach of data as discussed in Section III P below.

   b. LAUSD's Protocol for a breach of private information outlines;

      i. Private Information data breach procedure

      ii. Notification of those responsible for managing any event

P. Breach of Private Information Procedure

A breach of private information is a serious matter. LAUSD staff and faculty and Central Office departments must make every reasonable effort to prevent breaches from occurring. In the event of a breach of personal privacy is identified or suspected in the use of a payment card, staff and faculty must reference this policy and ensure that all procedures are followed immediately to control the situation and would ensure that steps are taken to minimize the risk of a similar breach from happening again.

Step (1) Confirm and Contain

Confirm the validity of the suspected information breach. If the breach can be reasonably ascertained, containment should occur immediately. Containment includes, but is not limited to, disconnection of the host (e.g., server or other device) from the network or shutting down an application.

Care should be taken not to destroy data, but to preserve it without any form of network connection. Reconnection of the device to the network is not allowed until such time as remedial steps have been completed and re-connection is specifically approved by the Network Operations team or LAUSD's Chief Information Security Officer.

Step (2) Report

The following individuals are required to be informed as soon as possible:

a) LAUSD's Chief Information Officer
b) The Chief Officer in the chain-of-command for the affected area
c) The Office of General Counsel

A report coordinated and drafted by the Director of General Accounting, should indicate whose personal information was disclosed, to whom it was disclosed, when it was disclosed, how it was disclosed/accessed, and what steps have been taken in response to the disclosure.

Step (3a) Retrieve

Any documents or contents of electronic documents that have been disclosed to, or taken by, an unauthorized recipient should immediately be retrieved and secured (electronic documents or paper documents in facsimile form or printed email messages) or taken offline.

Documents, in any form, should not be destroyed until specific instruction is received. This may require personal attention to secure the documents and return them to their original location, remove them permanently from electronic storage or send them to the intended authorized recipient.

Step (3b) Remove

Private information taken offline (Step 1 and Step 3a) may still be accessible and discoverable on the Internet via Internet Search engines (e.g., Google). The usual time periods for information to be removed by the search engines through routine web crawling techniques is too elongated (e.g., weeks) and requests must be made to remove the information from search engine indexes and cache directly to the Internet Search engines companies. These requests must be made as quickly as possible. However, removal of data should not occur without the involvement of OGC and or the Los Angeles School Police Department, as it could be evidence in an investigation.

Support request procedures for the major search engines at the time of this document's creation are available as links below. This step, if necessary, will be coordinated under the direction of the Chief Information Security Officer.

Internet Search Engines: Clearing the index and Cache

- Google: http://www.google.com/intl/en/webmasters/remove.html
- Internet Search Engines: http://searchenginewatch.com/
- Bing: https://www.bing.com/webmaster/help/bing-content-removal-tool-cb6c294d
- The Wayback Machine, Internet Archive: http://www.archive.org/about/faqs.php#2
- Yahoo: https://help.yahoo.com/kb/search/SLN2214.html?impressions=true

Step (4) Notify

In cases where the breach results in the disclosure of personal information, California law may require that the affected individual(s) be notified.

Determination of reporting requirements will be made by the Office of the General Counsel on a case-by-case basis. The notification message and timing will be handled by the Office of the General Counsel exclusively – all personnel that are aware of a breach or that may be working on matters related to a breach must direct all communication regarding a breach back to the Office of the General Counsel.

LAUSD will follow the guidance on Notification and Communication as outlined by the Federal Trade Commission:

https://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/volumeii.pdf and California's Reporting Requirements for a Security Breach Involving Personal Information:

https://oag.ca.gov/privacy/databreach/reporting

Step (5) Investigate

LAUSD's Office of the General Counsel, the Chief Information Officer, and the Network Operations department will coordinate the investigation of any breach, for the purpose of determining and recording all the relevant facts concerning the breach and making recommendations. The objectives of this investigation include:

- a review of the circumstances surrounding the event as well as the adequacy of existing policies and procedures in protecting personal private information
- the impact of the breach and identification of all the individuals that were affected
- the actions that need to be taken to resolve immediate exposure, identification of vulnerabilities and steps to ensure future prevention

Step (6) Management Review

The Office of General Counsel and Chief Information Officer will document and report the detail of the breach of privacy and remedial steps to the Superintendent of Schools.
Any proposed exceptions to this Policy must be approved in writing by the Office of the General Counsel and Chief Information Officer, or their successors or designees. LAUSD and Related Entities shall comply with any procedures, manuals, memoranda, directives, and the like that relate to this Policy and were issued prior to or following the effective date of this Policy. Except for modifications, supplements or updates necessitated by changes in law, regulations, or administrative requirements; or for consistency with other LAUSD policies, the Superintendent or his/her designee will approve any proposed amendments to this Policy. The Division of Accounting and Disbursement will be responsible for the periodic review of this Policy, as well as ensuring that all appropriate parties are informed of any changes.

RELATED RESOURCES:

- Bulletin 1077.2, LAUSD Office of the General Counsel Information Protection Policy
- Bulletin 1553, Security Standards For Networked Computer Systems Housing Confidential Information
- PCI Data Security Standards: https://www.pcisecuritystandards.org/
- PCI DSS Document Library: https://www.pcisecuritystandards.org/document_library
- PCI-DSS v3.2.1: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf
- PCI-DSS Requirements and Self-Assessment Questionnaires: https://www.pcisecuritystandards.org/document_library?category=saqs#
- PCI Validated Approved Scanning Vendors: https://www.pcisecuritystandards.org/assessors_and_solutions/approved_scanning_vendors
- PCI Validated Qualified Security Assessors: https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors
- List of third-party service providers per Visa that are PCI Compliant: https://www.visa.com/splisting/searchGrsp.do

ATTACHMENTS:

Attachment A – Definitions
Attachment B – Merchant Level
Attachment C – Merchant Level Requirements
Attachment D – Self-Assessment Questionnaires (SAQs)

ASSISTANCE:

For assistance or further information please contact Accounting and Disbursement at ElectronicPayment@lausd.net