**ANNUAL PCI COMPLIANCE CHECKLIST**

|  |  |  |
| --- | --- | --- |
|

|  |
| --- |
| If you are using a device other than the Point-of-Service (POS) terminal approved by LAUSD, which is a JP Morgan Chase – Desk 5000, you must complete an annual PCI Self-Assessment Questionnaire (SAQ): <https://achieve.lausd.net/cms/lib/CA01000043/Centricity/Domain/849/8%20PCI-DSS-v3_2_1-SAQ-B_IP.pdf>(Examples of other POS devices include PayPal, Stripe, and Square but any device other than JP Morgan Chase’s product will necessitate that you follow the additional requirements outlined by the Payment Card Industry (PCI) Security Standards Council (SSC))Your response with all supporting documentation is **due each year by November 9.**If you need assistance, please email electronicpayment@lausd.netRequirements for users of the JP Morgan Chase terminalsRequirements for users of the other terminalsDocuments - Descriptions and Templates**SAQ Checklist:**Track your progress on this checklist to prepare for your SAQ submission and get a brief description of each item.1. **Departmental Credit Card Security Policy:**

This document outlines the policies and procedures put into place by your department to protect cardholder data. If a solution other than JP Morgan Chase is used, a Security Policy is required to address PCI DSS for your specific environment. You can use this template to create a Security Policy that is tailored to your specific needs. If you are using the JP Morgan Chase product, you do not need to complete this template. [Click here to download the Departmental Credit Card Security Policy template](https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fachieve.lausd.net%2Fcms%2Flib%2FCA01000043%2FCentricity%2FDomain%2F849%2F1%2520PCI%2520Departmental%2520Credit%2520Card%2520Security%2520Policy%2520Template%2520v3.2.1.docx&wdOrigin=BROWSELINK).1. **Breach of Private Information Procedure:**

This document prepares your unit for efficient action and communication in the event of a suspected or confirmed breach of a physical, or digital environment. This document is an Attachments included as part of the LAUSD Electronic Payment Policy. In the event of a breach, you are expected to follow this procedure. All users of POS devices are expected to follow this procedure in the event of a breach regardless of the issuing bank. [Click here to download the Breach Procedure](https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fachieve.lausd.net%2Fcms%2Flib%2FCA01000043%2FCentricity%2FDomain%2F849%2F2%2520Breach%2520of%2520Private%2520Information%2520Procedure%2520-%2520Appendix%2520E.docx&wdOrigin=BROWSELINK).1. **Training and Policy Certification:**

This document must be signed by the departmental Fiscal/Admin Officer and Department Head to certify that they commit to following the critical aspects of PCI and Merchant policies. In addition to certifying commitment to PCI training and policy, departments or schools that process electronic payment via credit and debit cards are expected to complete Security Awareness training via MyPLN. This document must be completed regardless of your POS issuing bank. [Click here to download the Training & Policy Certification template](https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fachieve.lausd.net%2Fcms%2Flib%2FCA01000043%2FCentricity%2FDomain%2F849%2F3%2520Annual%2520PCI%2520Training%2520and%2520Policy%2520Certification.docx&wdOrigin=BROWSELINK).1. **Service Provider List:**

This document lists all service providers (with contact info), including a description of service provided. Depending on the complexity of your environment, this could be as few as one service provider or many more dependent upon the service needs. Those using JP Morgan Chase terminals are not required to complete this document unless service providers are being used outside of any coordinated by Accounting and Disbursement. If you are not using a JP Morgan Chase terminal, you must complete this template. [Click here to download the Service Provider List template](https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fachieve.lausd.net%2Fcms%2Flib%2FCA01000043%2FCentricity%2FDomain%2F849%2F4%2520PCI%2520Service%2520Provider%2520List.docx&wdOrigin=BROWSELINK).1. **Access Control Log:**

Documentation of people and positions that have access to your credit card environment and their access level. This document is provided for all devices regardless of the issuing bank.[Click here to download the Access Control List template](https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fachieve.lausd.net%2Fcms%2Flib%2FCA01000043%2FCentricity%2FDomain%2F849%2F5%2520PCI%2520Access%2520Control%2520Log.docx&wdOrigin=BROWSELINK).1. **Contract information for your Credit Card Vendor and/or Service Providers:**

You can request this information directly from your Service Providers or Procurement. If you are not using the JP Morgan Chase device, you will need this information for completing your annual self-assessment. 1. **Terminal Tamper Inspection:**

Proof that credit card terminal inspections are happening on a regular basis. All users are expected to utilize these tools to help with ensuring tamper-free operation of your terminal regardless of the issuing bank. [Click here to download the Terminal Tamper Checklist](https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fachieve.lausd.net%2Fcms%2Flib%2FCA01000043%2FCentricity%2FDomain%2F849%2F7a%2520PCI%2520Tamper%2520Checklist.xls&wdOrigin=BROWSELINK).[Click here to download the Terminal Inspection Log](https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fachieve.lausd.net%2Fcms%2Flib%2FCA01000043%2FCentricity%2FDomain%2F849%2F7b%2520PCI%2520Device%2520Inspection%2520Log.docx&wdOrigin=BROWSELINK).[Click here to download the Terminal Tracking Sheet](https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fachieve.lausd.net%2Fcms%2Flib%2FCA01000043%2FCentricity%2FDomain%2F849%2F7c%2520PCI%2520Terminal%2520Tracking%2520Sheet.xls&wdOrigin=BROWSELINK). |
|  |

 |



1. **PCI – DSS Self-Assessment Questionnaire:**

Self-Assessment Questionnaire (SAQ) B-IP includes only those PCI DSS requirements applicable to merchants that process payment card data via standalone, devices with an IP connection to the payment processor. This self-assessment document must be completed by anyone using a device other than the JP Morgan Chase terminal.
[Click here to download the PCI SAQ B-IP](https://achieve.lausd.net/cms/lib/CA01000043/Centricity/Domain/849/8%20PCI-DSS-v3_2_1-SAQ-B_IP.pdf).