California State University, Dominguez Hills

Information Technology Information Security Standards

Credit Card Handling Security Standards

Overview

This document is intended to provide guidance to merchants (colleges, departments, organizations or individuals) regarding the processing of charges and credits on credit and/or debit cards. The goal is to protect against exposure and possible theft of account and personal cardholder information that has been provided to CSU Dominguez Hills.

This standard applies to all CSU Dominguez Hills departments, faculty, staff, students, organizations and individuals who, on behalf of the university, handle electronic or paper documents associated with credit or debit card receipt transactions or accept payments in the form of credit or debit cards. The scope includes any credit or debit card activities conducted at all CSU Dominguez Hills locations.

If you are a college, department, organization or individual that in any way accepts, captures, stores, processes or transmits credit or debit card information (both electronic and non-electronic), or uses third-party service providers to do this for you, then this standard applies to you.

Department or College Responsibilities

1) Complete a CSU Dominguez Hills Annual Self Assessment PCI Questionnaire and forward it to the Information Security Office for review.
2) Ensure your credit / debit card processing terminal is truncating the credit card account number so that only the last 4 digits of the account number are visible. If it is not truncating, you must contact the Information Security Officer.
3) Only designated persons should handle sensitive cardholder data.
4) All documentation that contains sensitive cardholder data must be kept at all times in a secure area such as a locked file cabinet, desk drawer or office. Keys may be distributed only to a restricted number of designated individuals. Dual control is recommended for access to secured areas. Any locks must be rekeyed or replaced if suspected of compromise or in the event of a termination or transfer of a designated individual.
5) Do not store credit card information on desktop computers or on portable electronic media devices. If credit card information is received via e-mail, print a copy of the e-mail and then delete the e-mail from the computer.
6) Do not transmit credit card information via fax.
7) If credit card information is received via telephone or mail order, do not write information on anything other than an approved form to be used for such purpose. Black out the credit card number so that only the last 4 digits of the account is visible prior to storing this information.
8) Never store the sensitive cardholder data (3 digit code found on the back of the card).
9) Maintain department credit card security handling procedures that comply with the PCI DSS - In addition to complying with campus information security policy and standards, departments should establish procedures for physically and electronically safeguarding cardholder information. Exceptions to these policies and procedures may be granted with written approval from an appropriate administrator.
10) Communicate procedures to staff - Appropriate administrators should communicate the department credit card security handling procedures to staff and ensure that the "Credit
Card Handlers and Processors Responsibilities” section of this standard is followed for all personnel involved in credit card transactions.

11) Restrict access based on a business need-to-know - Access to physical or electronic cardholder data should be restricted to individuals whose job requires access. Appropriate administrators should establish appropriate segregation of duties between personnel handling credit card processing, the processing of refunds, and the reconciliation function.

12) Assign a unique ID to each person with computer access - Departments should ensure that a unique ID is assigned to each person with computer access to credit card information. User names and passwords may not be shared.

13) Background checks - Departments should perform applicable background checks on potential employees who have access to systems, networks, or cardholder data within the limits of CSU Dominguez Hills HR policy, union bargaining agreements and local law. If employees have access to one card number at a time to facilitate a transaction, such as store cashiers, background checks are not necessary.

14) Using imprint machines - Imprint machines need special handling as they display the full 16 digit credit card number on the customer copy. Departments should not use imprint machines to process credit card payments unless personnel have been authorized to do so, and processes exist to securely store and dispose of the information.

15) Report Security Incidents to the Information Security Officer - If staff or faculty know or suspect that credit card information has been exposed, stolen, or misused, this incident must be reported immediately to the Information Security Officer. The report must not disclose by fax or e-mail credit card numbers, three or four digit validation codes, or PINs.
Credit Card Handlers and Processors Responsibilities

Staff or faculty with access to credit or debit card holder data must not:

1) Acquire or disclose any cardholder's credit card information without the cardholder's consent including but not limited to the full or partial sixteen (16) digit credit card number, three (3) or four (4) digit validation code (usually on the back of credit cards), or PINs (personal identification numbers)

2) Transmit or request any credit card information by e-mail or fax. If someone e-mails their data, staff and faculty should make them aware that, for their own safety, they should not do this again. The email or fax should be destroyed as soon as possible.

3) Electronically store or record any credit card information in any electronic format (Excel files, databases, e-mail, etc.) unless they have been authorized to do so by the Information Security Officer.

4) Request, record, or store any of the magnetic stripe data or the credit card confirmation code (three digit on the back of many cards and 4 digits on the front of American Express)

Staff or faculty with access to credit or debit card holder data should:

1) Store all non-electronic, physical documents or storage media containing credit card information in a locked drawer, locked file cabinet, or locked office.

2) Store all non-electronic, physical documents or storage media containing credit card information in a locked drawer, locked file cabinet, or locked office.

3) Report immediately a credit card security incident to an appropriate administrator if they know or suspect credit card information has been exposed, stolen, or misused.

4) Store only essential credit card information. Any stored information must be destroyed in accordance with the campus Record Retention Schedule. All media used for credit cards must be destroyed when retired from use. All hardcopies must be shredded prior to disposal.

Responsibilities of CSUDH

- Provide a secure gateway (Touchnet) for purpose of transacting electronic payments and for data storage, as required for compliance with credit card company regulations and in compliance with the e-Commerce Server Compliance Requirements.

- Provide advice / tools to enable departments to clearly follow industry best practices access, firewalls, patches, data storage, passwords, encryption and security.

- Investigate suspected security breaches and coordinate the response with the appropriate credit card agency, affected customers, and law enforcement as needed (see Cardholder Information Security Program (CISP) Security Audit Procedures and Reporting).
Payment Card Industry Data Security Standards (PCI DSS)

The campus and all departments that process credit or debit card information must comply with the Payment Card Industry Data Security Standards (PCI DSS). This includes the acquiring, accepting, capturing, storing, processing or transmitting of credit or debit card data, in both electronic and non-electronic formats.

PCI DSS is a set of comprehensive requirements for enhancing credit card data security. The standards were developed by the PCI Security Standards Council\(^1\), and a single violation of any of the requirements can trigger an overall non-compliant status. Each non-compliant incident may result in steep fines, suspension and revocation of card processing privileges.

Although the primary focus of the PCI DSS is on web-based sales and processing credit card information via the Internet, there are other processes that allow systems to be Internet accessible which may expose cardholder information. Basic functions such as e-mail can result in Internet accessibility of a merchant's network. Therefore, all campus credit card merchants, including merchants transmitting via a terminal on a dedicated phone line, or other approved method of transmission must complete an annual self assessment survey and, if applicable, an internal scan and a remote external scan by a PCI DSS approved vendor.

Storing Credit and Debit Card Holder Data

Card holder data is any personally identifiable data associated with a cardholder. This can be an account number, expiration date, name, address, social security number, or Card Verification Value CVV2\(^2\).

Storage of credit cardholder data refers to both electronic (databases, spreadsheets, etc) and non-electronic (faxes, imprint machine slips, hand written forms, etc) data.

The best way to be in compliance with PCI DSS is by **NOT** storing credit card holder data if there is no business need to do so.

Additional; information regarding storage of credit and debit card holder information can be found in Appendix A.

**DEFINITIONS**

Application Server: The computer hosting the application with which the general end-users or point-of-sale (POS) terminals connect.

Credit Card Information: Any cardholder or card information accessed to initiate a credit or debit card transaction.

---

\(^1\) The PCI Security Standards Council home page is [https://www.pcisecuritystandards.org/](https://www.pcisecuritystandards.org/)

\(^2\) The Card Verification Value (CVV2) is three- or four-digit value printed on the front or back of a payment card. CVV2 refers to VISA card naming scheme, whereas with MasterCard it is called Card Validation Code (CVC2), or Card member ID by Discover, Card Identification Number (CID) by American Express.
Cardholder Information Security Program (CISP): A standard of due care for securing Visa cardholder data wherever it is located. Compliance is required of all entities storing, processing, or transmitting Visa cardholder data.

Credit Card Number: Any part or all of the unique number identifying the credit or debit card account for a financial transaction.

Credit Card Processing: Act of storing, processing or transmitting credit or debit cardholder data.

Credit Card Processor: A third party vendor who processes credit and debit card transactions, routes payments to the CSU Dominguez Hills accounts, charges discounts and adjustment fees and generates statements.

Database Servers: The computer storing the sales and / or credit and debit card numbers.

e-Commerce Application: Any internet-enabled financial transaction application, whether a buying or selling application.

Encryption: Scrambling data in a recoverable format.


Merchant Number: The unique number identifying the unit accepting credit or debit cards for transactions. This number is necessary to settle the credit and debit card transactions at the appropriate CSU Dominguez Hills financial institutions. It is also used to identify the specific merchant (departments, faculty, staff, students, organizations and individuals) on the cardholder’s monthly credit or debit card statement.

Online Credit Card Acceptance: Credit and debit card payments submitted via the web using a third party vendor’s software and passed onto the credit card processor for real-time authorization. The third party vendor securely accepts and stores cardholder and sensitive cardholder data in compliance with the credit card company’s security requirements.

POS System: Computer or credit card terminals either running as stand alone systems or connecting to a server either at a remote off-site location.

Sensitive Cardholder Data: Any personally identifiable data associated with a cardholder, including but not limited to account number, expiration date, name, address, or social security number, CVC2 / CVV2 validation code (a three digit number imprinted on the signature panel of the card), and data stored on track 1 and track 2 of the magnetic stripe of the card.

Swipe Terminal: POS credit or debit card terminals
Appendix A: Credit Cardholder Data Storage Requirements

The following table includes high level information regarding storage and protection of cardholder data.

<table>
<thead>
<tr>
<th>Element of Data</th>
<th>Is Storage Allowed</th>
<th>Is Protection Required</th>
<th>PCI DSS Requirement 3.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary Account Number (PAN)</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Cardholder Name*</td>
<td>YES</td>
<td>YES*</td>
<td>NO</td>
</tr>
<tr>
<td>Service Code*</td>
<td>YES</td>
<td>YES*</td>
<td>NO</td>
</tr>
<tr>
<td>Expiration Date*</td>
<td>YES</td>
<td>YES*</td>
<td>NO</td>
</tr>
<tr>
<td>Full Magnetic Strip</td>
<td>NO</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>CVC2/CVV2/CID</td>
<td>NO</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>PIN/PIN Block</td>
<td>NO</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Even when the storage of credit card holder data is necessary, only some data elements (from the front of the card) may be stored as long as they are protected. Protection of data means that it needs to be encrypted or otherwise made unreadable (PCI DSS Requirement 3.4). However the sensitive authentication data (from the back of the card) may not be stored.

Additionally, only some data elements may be kept for the charge back process, whereas others may not. Sensitive authentication data, such as CVV2, are used for charge back verification but must not be stored. The entire 16 digit Primary Account Number (PAN), which is also used in charge back verification, cannot be kept in an unprotected mode. Only the first 6 and/or the last 4 digits\(^3\) can be stored in this manner, because in this form, they are not cardholder data. For example:

- Name + Expiry Date + Service Code is not cardholder data because the PAN is not retained
- 1234 5678 9012 3456 + Name + Expiry Date is cardholder data because the PAN is retained; so everything must be protected
- 1234 56xx xxxx 3456 + Name + Expiry Date is not cardholder data because store the first 6 and the last 4 digits unprotected
- 1234 56xx xxxx 3456 + Name + CVV2 cannot be stored since sensitive authentication data is retained

The PCI DSS storage rules also apply to digital voice and fax systems. Digital voice systems are searchable, so if a recording contains sensitive authentication data (CVV2/CVC2/CID), it cannot be stored and must be cleaned. Restricting both physical and logical access to such voice systems is recommended. Fax paper records also need to have sensitive authentication data deleted. This can be easily achieved by using forms in which a section can be removed. If the fax system has memory, that too

---

\(^3\) The standard campus practice involves storing last 4 digits only
needs to have the sensitive authentication data erased. PCI DSS storage rules also apply to any third party providers that you use for outsourcing; so departments should ensure that they are PCI compliant as part of any contract.
Review/Approval History

<table>
<thead>
<tr>
<th>Date</th>
<th>Audience</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>6/30/09</td>
<td>CIO</td>
<td>Reviewed</td>
</tr>
<tr>
<td>6/30/09</td>
<td>CIO</td>
<td>Approved</td>
</tr>
<tr>
<td></td>
<td>Cabinet</td>
<td></td>
</tr>
</tbody>
</table>