Credit Card Merchant Operational Procedures and

Information Security Requirements

Summary Document

This document summarizes Cash & Treasury Procedure 4.0. The full procedure is distributed annually to all applicable credit card merchants.

Payment Information Collection and Storage:

- The following methods of collecting credit card payment transaction information, including cardholder name, card number, expiration date, or security code is **PROHIBITED**:
    - Through e-Mail
    - Through a University of San Diego website; and
    - Through a third-party service provider who has NOT validated their compliance with applicable Payment Card Industry Data Security Standards (PCI DSS) including PA DSS (Payment Application Data Security Standards) where applicable. All third-party service providers must provide current, applicable and appropriate Attestations of Compliance (AOCs), as prescribed by the PCI Security Council. See Third-Party Service Provider Requirements section below.

- The following types of cardholder data storage are **PROHIBITED:**
    - The storage of the full contents of any magnetic strip track (e.g. full track data)
    - The storage of the three or four-digit validation code on the back of a card; and
    - The storage of personal identification number (PIN) or encrypted
    - Personal identification number (PIN) or encrypted PIN block

Manual transactions, with physical authorization:

Physical credit card information shall be maintained in a secure location, accessible only to university personnel directly responsible for processing the transaction. The secure location may not be accessible by persons other than those immediately responsible for the collection and transaction of the payment, including night crews or other staff members. All physical media containing cardholder data can be identified as confidential. In addition, the credit card number and expiration date may only be stored for the shorter of ***the date of physical receipt to the date of the card payment transaction, or seven days.*** Credit card transaction information must be securely shredded upon the earlier of the two events above.

Credit card transaction information in whole or in part may **NOT** be stored on any personal computer, network drive, or by any other electronic method. Information may not be sent to on or off-campus storage facilities.

Electronic Commerce Transaction- Fully outsourced, No internal processing or transmitting:

This section applies to online credit card transactions performed directly by the **customer** using a PCI DSS validated third party service provider. No credit card transaction information will be handled by USD staff. Only third parties confirmed to be PCI DSS compliant annually may be contracted by the university to provide online payment capability.

See Contracting with Third-Party Service Providers below.

As Service providers are responsible for transacting e- payments, the university shall not maintain any information in physical or electronic format which would allow the transaction to be recreated. (see Payment Information Collection and Storage section above). Electronic format includes but is not limited to, email, Excel or Word document files, Databases, or other electronic means.

Point of Sale Systems Connected to the Internet, no electronic cardholder data storage:

Point of Sale (POS) transactions are typically card-present and are connected to the internet to transmit cardholder data.

See Contracting with Third-Party Service Providers below.

POS systems may not store cardholder data on any computer system or network installed within the university's computing environment.

All replacements, additions, alterations, or other configuration changes must be approved by Finance and Enterprise Administrative Systems and Services.

On-line Payment Applications, Virtual Terminals and or Back-End Payment Systems:

Systems used to process or transmit cardholder data on behalf of a customer, including CRM (Customer Relationship Management), Assisted Payments, or other staff-processed payments fall into this category. No credit card transactions may be transmitted by USD staff on a device that is not Issued by Finance, and/or configured by and monitored by the appropriate USD IT department.

Cardholder data may ONLY be transmitted:

- Using a P2P (Point to Point) Encryption hardware device, issued by Finance and assigned to a specific operating unit

Use of Wireless Terminals:

Wireless terminals must be authorized by Finance, provided by the university's acquiring merchant bank, and terminate directly to the processor. The use of AP network-based devises is PROHIBITED. Wireless transmission of cardholder data other than through a devise as described above is prohibited. All cardholder data environments MUST be isolated from university wireless data points.

Credit Card Transaction Processing

A cardholder signature is required for credit card payments received by secure fax, US postal service mail, or hand delivered for staff processing via a manual credit card terminal.

Further, no full card numbers may be retained after the transaction is complete. See Payment Information Collection and Storage section above.

Transaction receipts may not include the card expiration date or three or four-digit security codes located on the back of the card.

Transaction Receipt and Summary Retention

Transaction Receipts or other documentation may not include the full card number, also known as the Primary Account Number (PAN). PANs must be truncated on all receipts retained by the university or delivered back to the customer, showing the last four digits only. Further, no full card numbers may be retained after the transaction is complete.

Transaction receipts may not include expiration date or the three or four-digit validation code located on the back of the card.

Contracting with Third-Party Service Providers:

All Service Providers with access to cardholder information must:

- Be approved by Finance
- Be contractually obligated to maintain the appropriate PCI and/or PA (Payment Application) DSS compliance, and provide USD with the appropriate Attestation of Compliance (AOC) at least annually and upon request
- Expressly acknowledge their responsibility for the security of cardholder data they transmit, process, store or otherwise handle in any manner or for any length of time in the contract, agreement or addendum to the contract or agreement.

- Payment Applications subject to PA DSS must be listed as validated by the PCI Security Council as a Validated Payment Application. Validation must refer to exact product and version used by the university.

Adherence to Web Privacy and Responsible Computing Polices

All credit card merchants must remain in compliance with USD's Web Privacy and Security Statement and policy on Responsible Use of University Computing Resources
http://www.sandiego.edu/legal/policies/community/technology/computing.pdf

Point of Sale Terminals and Database Security

POS providers must comply with PCI DSS in addition to PA DSS (Payment Application Data Security Standards) where applicable. See Third-Party Service Provider and POS information above.

Credit card merchants with POS databases hosted by USD must undergo regular scans through the university's PCI DSS qualified scan provider. Scan parameters must be reviewed annually or when database configuration changes occur.

All POS cashiers must be trained annually and certify their receipt of training. Departmental merchant directors are responsible for obtaining and maintaining cashier training.

Other Security Matters

All changes to merchant card environments, including the transition from manual terminal processing to electronic commerce processing, must be coordinated through Finance.

No cardholder or transaction information may be downloaded onto any university or other network, hard drive, server, or other electronic facility.

USD directors over areas involved in credit card merchant activity are responsible for the actions of any consultants hired to service electronic or other credit card payments. Directors are also responsible for the adherence to the procedures referenced here, and all specific procedures in Pr.4.0, all applicable PCI departmental Merchant Guidelines regarding credit card processing and university policies. Access to cardholder information and transaction information, as well as the university's networks and systems must be limited to necessary access only.

All credit card merchants must annually certify their compliance. The appropriate PCI Data Security Questionnaire (SAQ Form A, B, C or D) must be completed for each merchant account. Departmental merchants may be asked to complete questionnaires, checklists, or answer questions regarding their

operating environment. All "in-scope" websites, hardware, software, databases or other must undergoing network scans if required based upon operational configuration.

Information Security Compromises

Credit card merchants and service providers must immediately report the suspected or confirmed loss or theft of any cardholder data, credit card material, records or other information.

If a USD staff member knows or suspects a security breach with a credit card merchant or service provider, the staff member must take immediate action to limit the exposure of further data and report the incident to the USD Office of Public Safety. Note: If a Visa member fails to immediately notify VISA USA Fraud Control of the suspected or confirmed loss or theft of any VISA transaction information, the member will be subject to a penalty of $100,000 per incident. In addition, the university could be subject to fines up to $500,000 per incident for any merchant or service provider that is compromised at the time of the incident.

In the event of a security intrusion:

- Contact the Office of Public Safety immediately at extension 7777 if report is after hours
- Notify the Office of Finance at compliance@sandiego.edu and at 260-2248, who will then notify and coordinate with Information Technology Services, the acquiring merchant bank, third party providers and Visa, MasterCard, Amex and Discover as appropriate if report is during business hours
- Contain and limit exposure by:
    - Preventing access or the alteration of compromised systems (e.g. do not log in or change passwords, do not log in as ROOT);
    - Isolate the compromised machine from the network by unplugging the network cable while leaving the machine's power on;
    - Preserving logs and electronic evidence;
    - Documenting all actions taken with time and date; and
    - Being on high alert and monitoring all systems.

Change Log:

E. Brown July 2011 E. Brown June 2013 E. Brown April 2014 G. Proctor June 2017

G. Proctor April 2024