Credit Card Merchant Operational Procedures and Information Security Requirements

Scope

This procedure covers the operational procedures and process for maintaining compliance with the Payment Card Industry Data Security Standards (PCI DSS). See University General Guidelines Document at ***Appendix G****.*

System References

Manual Credit Card Terminal*- non-integrated, stand-alone credit card terminals*

Electronic Commerce *Sites accepting credit cards provided by PCI compliant third Party Service Providers on behalf of the university*

Point of Sale (POS) *systems with integrated credit card capability*

All university networks, hard drives, servers, and other computer systems where credit card information is processed or transmitted from are considered "in scope" for PCI compliance, and must be approved by ITS and Finance. NOTE that electronic storage of Primary credit card Account Numbers (PANs) is prohibited by University General Guidelines.

University General Guidelines

See **Appendix G** for the University's General Guidelines on Credit Card Processing.

Responsibility

Directors or Deans are responsible for university credit card merchant operations within their Departments. University Credit Card Merchant defined as:

- Any university department with a merchant identification number issued by Finance
- Any university department accepting credit card information as a form of payment to be processed via a university process
- Any university department receiving payment by credit card through a third party, or receiving payment from a third party accepting credit card payments on the university's behalf (outsourced merchant accounts included)

Credit Card Merchants include, but are not limited to:

- Any university department collecting revenue via credit card payments described above
- University departments utilizing the Central Portal process (coordinated through Finance)
- University departments utilizing any payment solution through the university's official E-commerce and cashiering solution provided by cashNET or Target X Registration system
- University departments with access to cardholder data, regardless of transmission, process or storage

Operational staff is responsible for the daily operations and maintenance of the credit card terminal, deposit information and reporting as assigned by Director or Dean.

Distribution

All University Credit Card Merchants

Accounting

Finance

Information Technology

Ownership

Finance will guide annual compliance verification with these procedures and University General Guidelines.

Procedure Purpose

These University Procedures and General Guidelines formalize the best practices to achieve compliance with all applicable PCI DSS Requirements and internal controls for all credit card merchants associated with the University of San Diego.

The following Procedures set standard best practices and internal controls related to cardholder data security as it relates to credit card transactions processed by or on behalf of the university. The standards set forth in these procedures meet the Security requirements of the **Payment Card Industry** or PCI (Visa, MasterCard, American Express and Discover Associations) standards.

The PCI has published 12 general standards that all Members, merchants and service providers with access to cardholder data must comply with.
The standards address six general categories:

1. Build and Maintain a Secure Network
2. Protect Cardholder Data
3. Maintain a Vulnerability Management Program
4. Implement Strong Access Control Measures
5. Regularly Monitor and Test Networks
6. Maintain an Information Security Policy

See Visa's website for complete description.
https://usa.visa.com/support/small-business/security-compliance.html

The university is required by the Payment Card Industry (PCI) to ensure all university credit card merchants are compliant with the **PCI Data Security Standards** (PCI DSS) to avoid various categories of significant fines and reduce the risk of information breeches.

COMPLIANCE
Compliance with this Procedure, University General Guidelines and other related Guideline Documents is mandatory.

Coordination of the annual assessment process is be performed by Finance. Periodic audits will be performed by Finance to ensure that Departmental Merchants are in compliance with applicable PCI DSS requirements.

All personnel with designated credit card merchant responsibilities or staff who have been delegated limited or other access to cardholder data will receive PCI DSS training annually. See Annual Training Requirement below.

NON-COMPLIANCE
Non-compliance with these procedures may result in loss of departmental merchant credit card capabilities. If non-compliance is unveiled during a periodic audit or an annual assessment, a remediation plan will be created and must be implemented within 2 months of remediation dissemination.

In general, if a Departmental Merchant fails to meet the expectations of the remediation plan, credit card processing capabilities will be revoked.

ANNUAL TRAINING REQUIREMENT
All USD staff with access to cardholder data (Departmental Merchants) shall receive training at least annually. All Departmental Merchants shall acknowledge that they have received training on PCI DSS requirements and understand those requirements applicable to their operation.

Forms of Acknowledgement may include:

1. **Appendix F** of Cash & Treasury Procedure PR.3.0 Credit Card Merchant Operational Procedures
2. Sign in at Annual Departmental Merchant Training and/or submission of Qualifying Self-Assessment Questionnaire and Certification of Training Video
3. Signed Departmental Procedure Acknowledgement (cashiers and casual workers)

DEPARTMENTAL PROCEDURE DOCUMENTATION REQUIREMENT
All USD departments with access to cardholder data (Departmental Merchants) must submit a copy of their ***written operating procedures***, along with their annual certifications to Finance. Procedures must include applicable credit card PCI DSS requirements, including the collection, transmission, processing, and retention of cardholder data.

University of San Diego PCI Compliance Statement:

Please refer to the University's General Guidelines on Credit Card Processing Statement at **Appendix G**

1.0 Payment Information Collection, Storage and Destruction:

1.01 Collection of Cardholder Data

1.01.1 The following methods of collecting credit card payment transaction information, also known as cardholder data (CHD) including cardholder name, card number, expiration date, or security code is **PROHIBITED**:

- Electronic mail (e-mail)
- Any end-user messaging technology
- Physically unsecured fax
- Multi-function fax machine, connected to university networks, printers or other university systems
- Through a University of San Diego website
- Through a NON-CERTIFIED Third Party Service Provider. **PCI certification/VISA Validated Payment Application** must be provided to the university prior to contracting with provider. See Section 4.0 Third Party Service Provider Requirements below.

1.01.2 IF CHD is received in any Prohibited manner, the following steps must be taken:

1. Do NOT print (email, PDF attachment, fax notification on multi-function fax machines)
2. Do NOT process transaction
3. Reply to e-mail with the CHD ***deleted***, stating USD's Policy prohibiting receipt of cardholder data via email or by any unsecured method, and arrange for a secure transmission of CHD.
4. Delete email or fax notification from multi-functional fax machines and empty trash folder or fax history

1.01.3 Cardholder Data may be collected by the following methods:

- Mail
- Physically secure fax with dedicated telephone line
- Card present (swiped at a USD-approved credit card terminal)
- Original paper registration form
- By telephone

See **Appendix A** for collection form format

1.02 Storage of Cardholder Data

1.02.1 Storage of the following data in any form; physical or electronic is **PROHIBITED**:

- Full contents of any track from the magnetic strip, i.e. full contents of any track (from the magnetic stripe located on the back of the card, equivalent data contained on a chip, or elsewhere)
- 3 or 4 digit card-validation code on the back of a card
- Personal Identification number (PIN) or the encrypted PIN block

Prohibited electronic storage includes but is not limited to storage on any PC, network drive, or by any other electronic method.

1.02.2 Allowable cardholder data includes the Primary Account Number (PAN) and card expiration date, in addition to cardholder name, address and other contact information.

1.02.2.1 PAN is masked when displayed on receipts, reports, or other media.

1.02.2.2 Only personnel with a business need have access to the full PAN at any time.

1.02.2.3 Access to cardholder data is assigned based on individual personnel's job classification description and/or function

1.02.3 Allowable cardholder data collected in an approved manner must be securely stored. The secure location must be accessible only to university personnel directly responsible for processing the transaction. Cardholder data may not be accessible to persons other than those immediately responsible for the collection and transaction of the payment, including night crews or other staff members.

1.02.4 All physical media containing cardholder data can be identified as confidential.

1.02.5 Retention or storage of allowable cardholder data in a secure manner must be limited to the shorter of:

Time of physical receipt to Card Payment Transaction

Or

7 Days

Retention of cardholder data after the payment has been authorized is **PROHIBITED**.

1.02.6 No cardholder data, including full PAN shall be maintained by the university for electronic commerce transactions initiated by payer.

1.03 Destruction of Cardholder Data

1.03.1 Appropriate Disposal must occur upon the earlier of the two events above, and include

- Cross-cut shredded,
- Incinerated
- Pulped

1.03.2 Credit card transaction information in whole or in part may NOT be sent to on-campus or off-campus storage facilities

1.03.3 Responsible Departmental designee must perform and document a quarterly review of location described in 1.02.3 to ensure that cardholder data is not being retained in excess of the allowable retention period per 1.02.5 above.

2.0 Credit Card Transaction Transmission and Processing

2.01 Processing Cardholder Data

2.01.1 All third parties service provider, including software or internet application providers with access to cardholder data must be secure and confirmed to be PCI Compliant. See 4.0 Third Party Provider Requirements below

2.01.2 All payment processing must occur within the time frame described in section 1.02.5 above

2.01.3 Applicable general guidelines for departmental merchants published and disseminated by Finance must be followed and may include:

- Operating Guidelines for:
  - SAQ- Validation **Type A** Merchants
  - SAQ- Validation **Type B** Merchants
  - SAQ- Validation **Type C** Merchants
  - SAQ- Validation **Type D** Merchants
  - Pr 3.1002 CASHnet User Procedures
- Special Notices from Finance regarding Payment Processing Updates
- Updated Procedure Documents surrounding payment processing

2.02 Transmission of Cardholder Data

2.02.1 Acceptable methods of transmission of cardholder data by University staff:

- A Manual dial-up credit card terminal, connected to a phone line and NOT connected to any other USD system
- A cellular-based "wireless" terminal, issued by USD's Acquiring bank through the office of Finance
- A Point of Sale terminal that is monitored under the Scope of PCI compliance by ITS and Finance
- A cellular devise configured and issued by USD's ITS department
- A PCI Locked Down terminal, specifically configured and issued by ITS and Finance

2.02.2 Use of USD's general Wireless Network and environment for transmission of cardholder data is PROHIBITED.

2.02.3 If cardholder data is moved, a log must be maintained to track all media that is moved from a secured area to a second secure area. Management approval must be obtained prior to moving the media (especially when media is distributed to individuals).

2.02.4 Logs of moved media must be submitted to Finance with annual PCI Compliance validation materials for audit.

3.0 Departmental Merchants

3.01 Departmental Procedures

3.01.1 Departmental procedures must be published and disseminated by merchant department management, and include all applicable PCI requirements and other operating procedures surrounding credit card processing.

3.01.2 Procedures must be followed and include but are not limited to:

- Cashier's Training Guides
- Cashier's Procedural Documents
- Staff Payment Processing Procedures
- Departmental Operating Procedures

3.02 Manual Transaction with Physical Authorization Merchant

PCI Requirement: PCI Data Security Standard Self-Assessment Questionnaire B 3.1 (29 applicable requirements)

3.02.1 Eligibility under 3.02 requires that the department uses only a standalone, dial-out terminal or cellular-based "wireless terminal", not connected to the internet or any other system within the University's environment, including the wireless network

3.02.2 Department must be in **c**ompliance with:

- All sections of this procedure document
- **Operating Guidelines** version SAQ- Validation **Type B** Merchants

3.02.3 Dial up or cellular terminals must be settled daily. The batch total from the daily settlements are sent to Treasury each month. It is the merchant department's responsibility to reconcile what is posted to the general ledger; any discrepencies must be reported to Treasury in a timely basis. Cashier deposit must include a Departmental Credit Card Reconciliation form (DCCR) in addition to Cashier's deposit form

3.03 Electronic Commerce Transactions- Fully Outsourced Merchants

PCI Requirement: PCI Data Security Standard Self-Assessment Questionnaire A 3.1 (13 applicable requirements)

3.03.1 Eligibility under 3.03 requires that

- Department relies completely on the third party service provider for credit card processing and storage
- E-payments are made exclusively by payer, and no cardholder data is handled by university staff

- Customers MUST be directed to use "Any Computer with an Internet connection" to transact self-serve payments
- Customers may NOT be directed to a specific or designated university computer

3.03.2 Department must be in compliance with

- All sections of this procedure document
- Operating Guidelines version SAQ- Validation **Type A** Merchants

3.03.3 Online credit card transaction information is transmitted directly by customer directly to a PCI Certified Third Party Service Providers/VISA Validated Payment Application only. Only third parties confirmed to be a PCI Compliant/VISA Validated service provider may be contracted by the university to provide online payment capability.

3.03.4 As Service providers are responsible for transacting e- payments, the university shall not maintain any information in physical (see above) or electronic format, which would allow the transaction to be recreated. Electronic format includes but is not limited to, Excel or Word document files, Databases, or other electronic means. See Section 4.0 for Third Party Service Provider requirements

See Virtual Terminal Requirements at 3.05 below.

3.04 Point of Sale (POS) Systems Connected to the Internet, no Electronic Storage of Cardholder data

PCI Requirement: PCI Data Security Standard Self-Assessment Questionnaire C 3.1 (80 applicable requirements)

3.04.1 Eligibility under 3.04 requires that

- Credit card transactions are processed using a point of sale, the card is present at the time of transition, and the POS is connected to the internet to transmit cardholder data
- All POS service providers with access to cardholder information must be contractually obligated to maintain PCI compliance, expressly acknowledge responsibility for cardholder data, and provide USD with validation of compliance

3.04.2 Department must be in compliance with

- All sections of this procedure document *AND*
- Operating Guidelines version SAQ- Validation Type C Merchants *OR*
- Operating Guidelines version SAQ- Validation Type D Merchants

3.04.3 Point of Sale Requirements:

- POS systems may not store cardholder data on any computer, database, network or other system installed within the university's computing environment
- All POS systems and database hosted by the university must undergo quarterly scans performed by independent, Qualified Scanning Vendor

- Vendor- hosted database providers must provide annual Attestations of Compliance of vendor's PCI compliance status to the university
- Vendor-hosted database providers must provide quarterly scan reports indicating a pass external scan by an approved scan vendor
- Maintain current version-specific compliance with, PA DSS as per the PCI Council website list of PA DSS providers
- See section 4.0 for Third Party Service Provider requirements

3.04.4 User Names and Passwords:
All users must login with a unique login and password, allowing every transaction to be traced to an individual user. Shared logins and passwords are **PROHIBITED**.

3.04.5 Cashier /User Operating Requirements:

1. Cashiers or users must log out of the system when not in use
2. Cashier or user shall NOT use or login as another user
3. Cashier or user shall NOT allow another user access a POS or virtual terminal when logged in

3.04.6 POS Department Procedures Must include the following:

1. User ID restricts access to least privileges necessary to perform job functions. Privileges within the POS systems must be assigned to individuals based upon job classification and function, and automatically controlled. Access is structured to "deny all" unless express access is granted by authorized administrator. (note: configuration assistance may be required by Database and/or System ITS Administrators.)where was
2. Additions, deletions or other modifications of user IDs, credentials, and other identifier objects are controlled so that each user ID is implemented only as authorized. Appropriate identification must be made by administrators before password resets can be granted.
3. Administrators must reset passwords to a unique value for each user, and each user must be required to change their password immediately after the first use.
4. Access for terminated users must be immediately deactivated or removed.
5. Approval for access to cardholder data must be authorized and documented.

3.04.7 Authorized Dean/Director Responsibilities:

1. Enforcement of applicable PCI DSS requirements
2. Documentation of Operational Procedures that address all applicable PCI DSS requirements
3. Ensure annual training for all system users or others with access to cardholder data

3.05 E-Commerce Gateway, Virtual Terminal used to transmit Cardholder data to Secure Processor, including any transmission of cardholder data by USD staff on behalf of a customer. On-line payment applications, including virtual terminals, back-end payment systems used to process or transmit cardholder data

PCI Requirement: PCI Data Security Standard Self-Assessment Questionnaire C 3.1 (80 applicable requirements if single location) or SAQ D (286 applicable requirement if multiple locations.

3.05.1 Eligibility under 3.05 requires that

- No cardholder data may be transmitted from a regular university PC
- Cardholder data MUST be transmitted via a PCI Locked Down terminal, directly to a secure Gateway or Processor
- Customers MUST be directed to use "Any Computer with an Internet connection" to transact self-serve payments
- Customers may NOT be directed to a specific or designated university computer

3.05.2 Departments must be in compliance with

- All sections of this procedure document
- Operating Guidelines SAQ- Validation Type C Merchants
- Pr 3.1001 E-Commerce, Event Payments- Checkout or Storefront (if applicable)
- Pr 3.1002 CASHnet User Operating Procedures (if applicable)
- All E-commerce Gateways as described above must undergo quarterly scans in addition to completion of the annual SAQ C or D. Verification of PCI compliance by payment service provider (eg. Paypal, Authorize.net, CyberSource) is required. See Virtual terminal requirements below.

3.05.3 User Names and Passwords:

- All gateway users must login with a unique login and password, allowing every transaction to be traced to an individual user
- Shared logins and passwords are PROHIBITED

3.05.3 User Operating Requirements:

- Cashiers or users must log out of the system when not in use
- Cashier or user shall NOT use or login as another user
- Cashier or user shall NOT allow another user access a POS or Virtual Terminal when logged in

3.05.4 Departmental Operating Procedures must include:

- Virtual terminal or gateway user ID restricts access to least privileges necessary to perform job functions.
- Privileges within the virtual terminal or gateway must be assigned to individuals based upon job classification and function, and automatically controlled.
- Access is structured to "deny all" unless express access is granted by authorized administrator.
- Additions, deletions or other modifications of user IDs, credentials, and other identifier objects are controlled so that each user ID is implemented only as authorized.
- Appropriate identification must be made by administrators before password resets can be granted.

- Administrators must resent passwords to a unique value for each user, and each user must be required to change their password immediately after the first use.
- Access for terminated users must immediately be deactivated or removed.
- Approval for access to CHD must be authorized and documented in Departmental Operating Procedures.

3.05.5 Authorized Dean/Director Responsibilities:

- Enforcement of applicable PCI DSS requirements
- Documentation of Operational Procedures that address all applicable PCI DSS requirements
- Ensure annual training for all system users or others with access to cardholder data

3.06 See PCI Locked Down Terminal Configuration document

4.0 Third Party Service Provider Requirements

4.01 Approval of Third Party Service providers with access to cardholder data

All electronic commerce sites must be pre-approved by Finance and Information Technology. Approval must be obtained prior to:

1. Finalization of agreement or contract between the university and a third party provider
2. E-commerce site placed into production
3. Commencement of any electronic commerce.

4.01.1 Information Technology must approve final configuration and implementation of integrated electronic commerce sites

4.01.2 All Third Party Service Providers with access to cardholder data, regardless of inclusion on PCI Security Council List of Validated Payment Application list, VISA or MasterCard Validated Service Provider lists shall be approved by Finance and Information Technology before they can be engaged

*See current E-commerce website Authorizations form at **Appendix D** and Events Payments E-commerce Authorization form at **Appendix D-1***

4.02 Confirmation of PCI Compliance

The appropriate PCI documentation must be determined.

- Non-implemented solutions (no hardware, software or other system integration with third party solution) are providers of web-accessible solutions, not connected to any other system within the university and hosted by the provider
  - Subject to PCI DSS Attestation of Compliance (AOC) validation
  - Subject to contractual obligations
  - Subject to quarterly verification of scan compliance (AOSC) validation
- Implemented solutions (hardware, software, databases or other, hosted by USD and/or integrated with other University systems) are providers of point of sale

terminals hosted by USD, or other software which has been installed on USD systems
- Subject to PCI DSS Attestation of Compliance (AOC) validation
- Subject to PA DSS (Payment application data security standards)
- Subject to contractual obligations
- Subject to quarterly verification of scan compliance (AOSC) validation

PCI compliance must be confirmed before Third Party Service providers are engaged. Confirmation must be ongoing and continuous, and occur no less than annually. Evidence of PCI compliance (VISA or MasterCard list) or Payment Application list (PCI Council), and/or either an Attestation of Compliance (AOC) signed by the appropriate authority to represent the Service Provider in PCI compliance matters or Report on Compliance (ROC) signed by a qualified security assessor (QSA) must be obtained before a contract is executed.

See **Appendix B** for Service Providers subject to PCI DSS and/or PA DSS as of 6-25-12.

4.02.1 PCI DSS Third Party Service Provider Validation Requirements
- Must provide USD with and Attestation of Compliance (AOC), signed by the appropriate company authority for PCI or Report on Compliance (ROC) signed by a qualified security assessor (QSA)
- Maintain a current "compliant" status on one of the following:
  - Visa's Global Registry of Service Providers - PCI DSS Validated Entities,
  - The MasterCard SDP Program (Site Data Protection)- Compliant Service Providers
  - PCI Security Council's List of Validated Service Providers or PCI Security Council's List of Validated Payment Applications

4.02.2 Contractual Obligation

All agreements with Third Party Service providers with access to cardholder information must expressly state their compliance with PCI Data Security Standard requirements, and must acknowledge that the third party is responsible for security of cardholder data in their possession. Agreement must provide that third party will continue to treat cardholder data as confidential upon termination of the agreement between provider and the university.

See **Appendix D-2** for Contract Amendment in the event that original service provider contract is missing language to satisfy this requirement.

4.01.3 Ongoing Compliance Validation

Third parties with access to cardholder data must provide the university with validation of current compliance at least annually, and at the request of the university

4.03 Other Third Party Service Provider requirements

4.03.1 Third party sites must have separate development, test and production environments, with separation of duties between the three.

4.03.2 Production data (real credit card numbers) may not be used for testing or development purposes

4.03.3 The most recent updates or patches to Third Party service providers, including payment systems must always be installed or applied to the university's application

4.04 Administrative Access to Third Party Service Provider solution

4.04.1 All users must be identified with a unique user and password name before accessing system components where cardholder data is accessible. Group or shared accounts and passwords are not permitted.

4.04.2 All passwords must be changed and cannot be vendor supplied passwords. Passwords must be changed every 90 days for applications which allow users to process transmit or view cardholder information.

4.02.3 Access for terminated users must be done immediately upon termination of revocation of credit card handling duties, and inactive user accounts must be removed by System administrator every 90 days.

5.0 Use of the University's Wireless Network is Prohibited

5.01 Wireless-Capable terminals must be

1. Authorized and provided by the university's acquiring merchant bank, and terminate directly to the processor and use CELLULAR technology OR
2. Authorized and provided by USD ITS, specifically coordinated to bypass the University's general wireless network

5.02 The use of USD AP network based devices is PROHIBITED

5.03 All cardholder data environments MUST be isolated from university wireless data points

6.0 Adherence to Web Privacy and Responsible Computing Polices

It is mandatory that all credit card merchants are in compliance with USD Web Services Privacy and Security Statement and The Policy on Responsible Use of University Computing Resources.

These Procedures and the General Guidelines do not replace, or supersede the USD Web services Privacy and Security Statement, dated June 1, 2005. Credit card merchants must be in compliance with the Security Statement at all times. Policy on Responsible Use of University Computing Resources

See http://www.sandiego.edu/legal/policies/community/technology/computing.pdf for University Policy and http://www.sandiego.edu/privacy/ for Privacy Statement.

7.0 Point of Sale Terminals and Database Security

7.01 All Point of Sale (POS) providers must comply with PCI DSS, and must be contractually obligated to maintain their PCI compliance and provide validation of such compliance to the university.

7.02 Requirements in 4.0 above apply to POS systems

7.03 Merchant departments with POS Databases which are hosted by USD must undergo quarterly scans through the university's PCI compliance validation provider. Scan parameters must be reviewed annually, or when database arrangements change

7.04 Requirement 1.0 and 2.0 above apply to databases. Cardholder information may not be stored in USD-hosted databases

8.0 Miscellaneous Information Security Items

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

8.02 No cardholder or transaction information may be downloaded onto any university or other network.

8.03 Directors of areas involved in credit card merchant activity are responsible for the actions of any consultants hired to service electronic or other credit card payments, and adherence to these procedures and all applicable University General Guidelines regarding credit card processing. Access to cardholder information and transaction information, as well as the university's networks and systems must be limited to necessary access only.

8.04 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.

8.05 All credit card merchant locations will have a director-level owner, and operational-level contact for which all communication regarding PCI and other information will be disseminated. Directors and operational staff will be responsible for merchant compliance.

8.06 All credit card information collection, including use of electronic commerce through third party service providers must be approved by Finance and Information Technology.

8.07 All Directors and operational staff, including replacements or new staff must sign the acknowledgement portion of this procedure upon taking over director or operator duties. See **Appendix F** for acknowledgement page.

9.0 Information Security Compromises

Members, service providers or merchants must immediately report the suspected or confirmed loss or theft of any material or records that contain Visa cardholder data. If a member knows or suspects a security breach with a merchant or service provider, the member must take immediate action to investigate the incident and limit the exposure of cardholder data.

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.

Members are subject to fines, up to $500,000 per incident, for any merchant or service provider that is compromised and not compliant at the time of the incident.

9.01 In the event of a security intrusion:

- If after business hours, contact the Office of Public Safety immediately at extension 7777
- If during business hours, contact Emergency Response Team immediately, and Finance will work with Information Technology, the acquiring merchant bank, third party providers and Public Safety as necessary. See **Appendix E** for Emergency Response Team Departments and current contacts.
- Contain and limit exposure:
    - Do not access or alter compromised systems (e.g., do not log on or change passwords; do not log in as ROOT).
    - Do not turn off the compromised machine. Instead, isolate compromised systems from the network (e.g., unplug the cable).
    - Preserve logs and electronic evidence.
    - Log all actions taken.
    - If using a wireless network, change SSID on the AP and other machines that may be using this connection (with the exception of any systems believed to be compromised).
    - Be on high alert and monitor all Visa systems.

Published: Finance

Date: June 30, 2005

Sources: PCI Security Standards Council
Visa, and Industry Cardholder Information Security Program
CampusGuard , USD's official Qualified Security Assessor
Ambiron TrustWave, Approved Independent Security Assessor

Application: ALL University of San Diego Credit Card Merchants

Updates: Updates will be issued annually, as PCI standards change, or as information in the Appendices change.

Update Log:

January 12, 2009	Erin Jow-Brown
April 5, 2010	Erin Jow-Brown
May 26, 2011	Erin Jow-Brown
July 25, 2011	Erin Jow-Brown
June 21, 2012	Erin Jow-Brown
June 27, 2013	Erin Jow-Brown
October 7, 2015	Ginny Proctor
July 11, 2016	Ginny Proctor
August 30, 2019	Ginny Proctor

Glossary

Payment Card Industry:	Refers to the Visa and MasterCard Associations, with regulatory authority over credit card processing and transactions. See Visa's website for complete description. https://usa.visa.com/support/small-business/security-compliance.html
PCI DSS Certification:	Attestation of Compliance: Required of all third-party service providers, web hosts, software application providers, application service providers and all other service providers with access to cardholder data at any point in transmission, processing or storage. Level 1 service providers, transacting more than 30,000 visa transactions annually must have an AOC signed by a Qualified Security Assessor (QSA) as part of the Report on Compliance (ROC) issued at the end of an on-sight assessment. AOC's must be provided at least annually and upon request. Attestation of Scan Compliance: Required of all third-party service providers, web hosts, software application providers, application service providers and all other service providers with access to cardholder data at any point in transmission, processing or storage. AOSC should be received on a quarterly basis. Registration on Visa's Global List of Validated Service Providers: As a best practice, registration and current status on this list should be maintained by all third party service providers with access to cardholder data. PA DSS PCI Validated Payment Applications: All third-party payment applications must be validated by the PCI Security Council prior to contracting with provider. NOTE: Acquiring banks will not approve a merchant account for use with a payment application without confirming the validation of the exact version and proposed installation. See PA DSS below.
PCI Security Standards:	The PCI DSS, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding

payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. Inc. International, to help facilitate the broad adoption of consistent data security measures on a global basis.

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

The PCI Security Standards Council will enhance the PCI DSS as needed to ensure that the standard includes any new or modified requirements necessary to mitigate emerging payment security risks, while continuing to foster wide-scale adoption.

Ongoing development of the standard will provide for feedback from the Advisory Board and other participating organizations. All key stakeholders are encouraged to provide input, during the creation and review of proposed additions or modifications to the PCI DSS.

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized:

Payment Card Industry (PCI) Data Security Requirements apply to all Members, merchants, and service providers that store, process or transmit cardholder data. Additionally, these security requirements apply to all “system components” which is defined as any network component, server, or application included in, or connected to, the cardholder data environment. Network components, include, but are not limited to, firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Servers include, but are not limited to, web, database, authentication, DNS, mail, proxy, and NTP. Applications include all purchased and custom applications, including internal and external (web) applications. *(Visa website* https://usa.visa.com/support/small-business/security-compliance.html*)*

See Appendix C for Official Standards Document

PA DSS:	Payment Application Data Security Standards- PA-DSS is the Council-managed program formerly under the supervision of the Visa Inc. program known as the Payment Application Best Practices (PABP). The goal of PA-DSS is to help software vendors and others develop secure payment applications that do not store prohibited data, such as full magnetic stripe, CVV2 or PIN data, and ensure their payment applications support compliance with the PCI DSS. Payment applications that are sold, distributed or licensed to third parties are subject to the PA-DSS requirements. In-house payment applications developed by merchants or service providers that are not sold to a third party are not subject to the PA-DSS requirements, but must still be secured in accordance with the PCI DSS.

APPENDIX A

Departmental or Event-Specific Registration/Payment/Event information

---

Credit Card Payment Information:

Please charge my credit card in the amount of $_____

Cardholder Name: (required) _____

Billing Street, City, State Address: _____

Billing Zip: (required) _____

Last four digits of card number __ __ __ __

Cardholder Signature: _____ **Date**:_____

I authorize the University of San Diego to charge my credit card as detailed below, for the total amount due detailed above.

……

Full Card Number: _____

Card Expiration Date ____/____/20___

Mo/ Day/ Yr

(The section below the dotted line of the registration form is to be destroyed upon completion of payment transaction, regardless of transaction success or failure, or 7 days after receipt by department, which ever is first. DO NOT RETAIN CREDIT CARD NUMBER AND EXPIRATION DATE.)

Mail or Fax Form To: University of San Diego
Department_____
5998 Alcala Park
San Diego, CA 92110
Hughes Admin. Bldg Rm.335

Secure fax 619-260-_____

DO NOT e-mail, e-fax, instant-message or otherwise submit electronically, as payment information received in this manner will NOT be processed

APPENDIX B

Current Third Party Service Providers subject to annual verification:

Blackbaud Payment Gateway	- PCI DSS
CBORD Payment Gateway	- PCI DSS
CVENT	- PCI DSS
CyberSource	- PCI DSS
Destiny Solution	- PCI DSS
HigherOne /cashNET	- PA DSS / PCI DSS
JSA Technologies	- PCI DSS
Micros 9700 3.6 MR6	- PA DSS
Nebraska Books	- PA DSS
Parkeon	- PA DSS / PCI DSS
PayPal Payment Gateway	- PCI DSS
Shift4	- PCI DSS
iModules	- PCI DSS
Target X	- PCI DSS
EventBrite	- PCI DSS
Handshake	- PCI DSS
UniCAS	- PCI DSS

All third party service providers and payment application providers with access to cardholder data must:

1. be contractually and expressly obligated to adhere to the PCI DSS requirements
2. be contractually obligated and provide written acknowledgement that the service provider is responsible for the security of cardholder data the provider possesses
3. provide annual Attestation of Compliance of the appropriate version
4. provide Quarterly Scan reports if applicable

APPENDIX C

See *Payment Card Industry Data Security Standards* attached at
https://www.pcisecuritystandards.org/security_standards/index.php

APPENDIX D

For NEW E-commerce Requests, contact compliance@sandiego.edu

APPENDIX D-2

Third Party Business Service Provider Application and/or Payment Application Provider Addendum Agreement

University of San Diego Department : _____

Business Application Description:

_____

_____

_____

Cardholder information is shared with third party service providers as part of the credit card payment process.

Vendor (the Company)	**Function**
_____	_____
	_____

1. All agreements between the University of San Diego and _____ *(the Company)* are subject to this addendum.

2. The Company acknowledges that _____ (the Company) is responsible for the security of cardholder data which it possesses, including during transmission, processing and/or storage.

3. The Company agrees to adhere to Payment Card Industry Data Security Standards (PCI DSS) requirements at all times, and to provide sufficient documentation supporting applicable PCI certifications. And, also provide the same PCI DSS compliance documentation for any Third Party Provider Company subcontracts with.

4. The Company agrees to provide annual Attestation of Compliance of the appropriate version, and quarterly Attestation of Scan Compliance to the university.

5. This agreement represents an addendum to the agreement between the above named vendor/service provider (the Company) and the University of San Diego.

Original Contract Date: (please attach original) _____

Vendor Acknowledgement

_____	_____
Company Authorized Security Signatory	Date
_____	_____
Printed Name	Title

APPENDIX E

Department	Departmental Contacts		
Finance			
	Steven Heath	x7594	compliance@sandiego.edu
	Ginny Proctor	x2434	compliance@sandiego.edu
ITS			
	Network Infrastructure Systems & Service, including CASHNet,		help@sandiego.edu
	iModules/Blackbaud Sphere,		crm@sandiego.edu
	Micros, CBORD, Nebraska, Shift4		auxts@sandiego.edu
Public Safety			
	All systems, during non-business hours		619-260-7777
Acquiring Merchant Bank			
	Patty White		patty.white@wellsfargo.com

APPENDIX F

I certify that I have received and reviewed University Cash and Treasury Procedure ***3.000 Credit Card Merchant Operational Procedures and Information Security Requirements*** document. I understand my responsibilities as a credit card merchant of the university.

Merchant Account number or Department Name: _____

_____ My operation is in compliance with this document as it relates to security of credit card information.

Or

_____ My area is out of compliance with this document with respect to the following processes:

_____
_____
_____
_____
_____

DEPARTMENTAL OPERATING PROCEDURES REQUIREMENT:
(PCI DSS Requirement 12: Maintain a policy that addresses information security for all personnel.)

_____ Our Departmental Operating Procedures dictating the handling of cardholder data and credit card payment processing are attached, and address all requirements applicable to my operation.

Responsible Director/ Authorized Signer

_____ _____
Signature Date

_____
Print Name

Responsible Departmental Operation User(s)

_____ _____
Signature Date

_____
Print Name

_____ _____
Signature Date

_____
Print Name

Please add additional page, if necessary, for all responsible departmental operations users.

Please submit with Training and Validation package to: compliance@sandiego.edu

APPENDIX G
GENERAL GUIDELINES: University of San Diego Credit Card Processing

Guideline Statement:
The university will comply with Payment Card Industry, Data Security Standards (PCI DSS) at all times. The university will comply with all reporting required by the University's acquiring merchant bank.

All credit card activity (sometimes referred to as "merchant card" activity) will be directed through Finance. All departments accepting credit card payments in any form are subject to these General Guidelines and all related University Credit Card Operating Procedures (UCCOP).

Guideline Implementation:
No Card Holder Data (as described by the Payment Card Industry), including Primary Account Numbers (PANs) shall be stored electronically. No PAN information shall be received or sent via e-mail or other non-secure method.

All third-party payment applications, vendors, service providers and processors utilized by the university who process, store or transmit cardholder Data (CHD) must be contractually obligated to meet all applicable Data Security Standards as prescribed by the Payment Card Industry Requirements and provide the appropriate and current Attestation of Compliance at least annually and upon the request by the university.

All university-initiated online transmission of CHD must be performed using a "PCI-locked down" computer terminal, or a USB-enabled Point-to-Point (P2P) peripheral device issued by the Office of Finance.

All departmental credit card merchants shall confirm their PCI compliance status at least on an annual basis. This process is described in the related UCCOP, and includes timely responses to inquires, questionnaires, checklists, and certification forms distributed by Finance. All merchants requiring quarterly scans shall be scanned by the university's official Approved Scan Vendor (AVS) quarterly.

Any indication of a breach of security involving CHD must be reported immediately. See UCCOP Pr.3000 for Incident Response Procedures.

Non-compliance with this Guidelines Document and/or all related UCCOP will result in the development of a remediation plan to be implemented timely. Failure to implement remediation plan may result in revocation of credit card processing capabilities.

Related University Credit Card Operating Procedures (UCCOP)
USD Cash & Treasury Procedures:

- 3.000 Credit Card Merchant Operational Procedures and Information Security Requirements.
- 3.1001 E-commerce, Events Payments- Checkout or Storefront AND 3.1002 CASHnet User Procedures
- Applicable Guideline document (SAQ-Validation Type A, B, C or D) PCI DSS Standards
- 12 General Requirements
- Directed Guideline or Notice Documents issued by Finance