CALIFORNIA STATE UNIVERSITY
FULLERTON

PCI DSS BUSINESS STANDARDS

September 1, 2016

OVERVIEW

CSU Fullerton is committed to maintaining a secure environment for credit card information, in compliance with the Payment Card Industry Data Security Standard (PCI-DSS), an industry security standard adopted internationally by the major payment card brands to protect credit card data, regardless of where that data is accepted, stored, transmitted or processed.

Individuals, departments, third-party contractors, or organizations operating on campus or under the name of the University may only accept credit cards on campus or through the web when expressly authorized to do so by the University's Controller's Office in coordination with the PCI Compliance Committee (PCICC).

The objective of CSU Fullerton PCI DSS Business Standard is to establish payment card requirements for all areas within the campus community that accept, process, transmit or store confidential cardholder information. The provisions of this policy and PCI DSS apply to the entire University, including its auxiliary organizations, as well as all third party vendors which support University credit card processing operations.

ROLES AND RESPONSIBILITIES

The campus CFO or his designee must approve of all physical locations, websites, 3rd party processors, or any channel accepting credit card payments. Credit card payments will only be accepted at approved locations, using an approved CSU merchant card processor.

The Controller's Office, in coordination with the University PCI Compliance Committee, is responsible for the implementation and oversight of this policy and general compliance with the PCI Standard, and:

- Establishing and closing merchant accounts. A merchant account allows businesses to accept payments by debit or credit cards;
- Establishing and maintaining relationships with the credit card payment processing providers and issuing banks;
- Approving any Point of Sale (POS) device or system to be used within the University;
- Defining the methods of transacting online payments on behalf of the University;
- Engaging a PCI Qualified Security Assessor (QSA) or Internal Security Assessor (ISA);
- Maintaining an inventory of all University departments that process credit card transactions using an approved University merchant account;
- Coordinating with Information Technology Division to review network segmentation configurations and other technical safeguards;

- Coordinating PCI training and security awareness programs;
- Enforcement of this policy and the PCI Standard including immediate suspension or termination of the ability to accept and/or process credit cards if a department fails to comply with this policy or the PCI Standard;
- Revocation of a merchant account immediately for failure to comply with this policy or the PCI Standard; and
- Other duties related to PCI Compliance as determined by the University.

CREDIT CARD ACCEPTANCE

The University is considered a merchant because it accepts payment by credit card for specific services or products. As a merchant, the University is required to follow the standards established by the Payment Card Industry Council. A merchant account is a relationship between the University and the University's bank account(s).

Cashiering sites accepting credit card payments should use only dedicated Point of Sale terminals or equipment supplied to the location by the campus' merchant card processor. All Point of Sale terminals and systems must be configured to prevent retention of the full magnetic strip, card validation code, PIN, or PIN Block cardholder data once a transaction has been authorized. If any account number, cardholder name, service code, or expiration date is retained, it must be encrypted and protected according to the standards outlined in the Payment Card Industry (PCI) Data Security Standards.

All University deployed gateways must operate in conformity with prevailing PCI Data Security Standards and must be compatible with the University's merchant card processor.

UNIVERSITY MERCHANT REQUIREMENTS

The following outlines general and technical requirements for all merchants who operate on behalf of the University where applicable:

- All merchants that accept payment cards on the University's behalf must be authorized by the Controller's Office and the PCICC. Please allow 4 to 6 weeks for processing requests.
- Merchant must complete the Merchant Identification Request form (MID) and submit to Controller's Office
- PCICC will review the questionnaire to ensure that merchant is PCI compliant
- All merchants must use processes and technologies approved by the Controller's Office and the PCICC.
- The University will not process any payment card transactions collected or submitted by unauthorized merchants.
- Only authorized merchants may use the University's resources to accept payment cards.

- All merchants must complete on an annual basis the University's PCI Compliance training provided through the Controller's Office.

- The Controller's Office/PCICC, as required, will annually file the appropriate Attestation of Compliance with its acquiring bank on behalf of all merchants of the University

- All merchants will review and update their business process environment, annually

The Controller's Office encourages University merchants who are pursuing ecommerce payments to utilize the Cashnet eMarket application. eMarkets merchants may not require a Merchant ID (MID).

Any fees associated with the acceptance of credit cards by a University department or organization will be responsibility of that entity. This may include, but not limited to, fees related to: credit card processing, eMarket set-up, infrastructure, security and administration.

Requests for or use of an MID or eMarket must include, but will not be limited to, the following requirements:

- Completion of Merchant ID application (not required for eMarkets);

- Annual review and update of BEQ;

- List of equipment and IP addresses or IP address range for webpay servers, payment application servers, cashiering workstation PCs, or EMV or P2PE stations;

- If applicable, completion of eMarket application;

- List of individuals with direct access to or control over credit card information;

- Completion of PCI training of individual(s) handling or processing credit card data;

- Attestation from merchant that they have read and understand the University PCI Policy for accepting credit card and/or eCommerce payments;

- Completion of Security Awareness training; and

- Acceptance of the University's Terms & Condition for handling, processing, transmitting, and storing credit card information

ELECTRONIC BASED CASHIER POINT OF SALE EQUIPMENT

All Point of Sale terminals and systems must be configured to prevent retention of the full magnetic strip, card validation code, PIN, or PIN Block cardholder data once a transaction has been authorized.

Therefore, the University requires:

- All cash registers and point of sale equipment must be PCI validated pin transaction security (PTS) device that is either EMV and/or Point to Point Encrypted (P2PE) solution;
- All KIOSK or PTS device, as part of KIOSK, must be inspected for any damage or tampered, on a daily basis
- Cash receipts issued contain a unique campus identifier assigned to each customer, with the PAN masked except for the last four digits or first 6 digits;
- The numbering mechanism providing consecutive transaction number control must be accessible only to the manufacturer's service representative or appropriate personnel who are independent of that cashiering station;
- Each cashier must be assigned a unique user ID, login, password, and cash fund not accessible by or shared with other individuals;
- All cash registers and point of sale equipment must produce session closeout audit totals for verification to receipts;
- All cash registers and point of sale equipment must require a supervisor's approval in order to process refunds or voids after a completed sale; and
- At the close of business, all portable POS equipment must be secured or stored in a lockable receptacle.

TRANSMITTING

University employees must be discrete and use common sense when handling cardholder data. Credit cards may only be accepted through the University in the following manner:

- In person (card present) using an approved PTS device (see Electronic Based Cashier Point Of Sale Equipment above); Credit card information must not be written down anywhere;
- Direct telephone contact (see NACHA guidance on TEL transactions); the constituent on the telephone should verify the payment card information twice; agents of the University should not read the payment card data back to constituent. Credit card information received must be entered directly to a validated PCI Secure Keypad device that is either an EMV and/or P2PE solution *or dedicated payment workstation*. Credit card information should not be written down anywhere; and

- As necessary, by physical mail (see manual request under Processing section).

Credit cards must **NOT** be accepted or sent in the follow manner:

- Via end user messaging technologies such as email, text message, SMS, chat etc. *(This information should not be forwarded or printed; the email should be deleted from your Inbox and Deleted Items folder; cardholder should be contacted and advised that this method of transmitting cardholder data is not secure and that we cannot process the payment)*; and

- Via fax, unless explicitly authorized by Controller for a defined business need and must only be through a secured dedicated fax machine that is password protected. This information should be immediately shredded in a crosscut shredder; cardholder should be contacted and advised that this method of transmitting cardholder data is not secure and that we cannot process the payment.

PROCESSING

The University has established the following safeguards related to the processing of credit cards:

- Cardholder Data received for manual processing (via mail, hand delivered, telephone) must be processed in an approved credit card merchant account the same day it is received;

- Manual requests to process a customer's credit or debit card must contain all of the following elements:

    - Properly signed/executed authorization from the cardholder (unless processing over the telephone as provided for in NACHA guidance on TEL transactions);

    - Credit/debit card account number with expiration date;

    - The card holder's correct billing address; and

    - Authorization codes, if the cardholder is not physically present.

  Cardholder data in written form must be redacted immediately following authorization;

- Acceptable forms of redaction are crosscut shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed;

- All credit card refunds must be processed back to the same credit card used for the original transaction. A different card may not be used;

- Primary Account Number (PAN) must be masked when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN;

- All ecommerce transactions must be processed through a PCI-DSS compliant automated system that is entirely hosted by a PCI DSS compliant service provider validated by the PCICC;

- All POS systems and/or "dedicated" workstations must be isolated from other University systems as authorized by the PCICC;

- Only "dedicated" workstations may be used to process credit cards. Any other uses of such systems must be approved by the PCICC;

- Stand-alone credit card terminals may process through analog phone lines or cellular service, but not through University wireless network; and

- Multi-factor authorization is required for personnel, via remote-access technologies, to access servers, processors, database, routers, etc., within the cardholder data environment.

- Remotely accessing cardholder data prohibits copy, move, and/or storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need

STORAGE

The University prohibits the storage of credit card data as follows:

- Authorized cardholder data (media), in hardcopy or electronic form;

- Sensitive Authentication Data (SAD); including the primary account number (PAN), expiration date and service code;

- Unprotected PANs must not be sent or received via any end-user messaging technologies (such as e-mail, instant messaging, and chat)

- Cardholder data on any portable devices including but not limited to USB flash drives, cellular phones, personal digital assistants and laptop computers; and

- Cardholder data in logs (for example, transaction, history, debugging, and error), history files, trace files or database contents.

Unopened mail must be stored in a secured location (locked safe, cabinet, room) accessible only by authorized staff. Locks must be changed whenever authorized staff separate from the University.

Hardcopy cardholder data may not be stored or retained unless approved by the Controller's Office. Once approved, all such data must be stored in a locked enclosure, such as a locked drawer, locked box, or safe. Only employees with a business need to access hardcopy cardholder data shall have access to the information.

DISPOSAL

University policy prohibits the storage of PAN or SAD without the approval of the Controller's Office. Any unneeded stored data must be disposed of immediately, in a certain manner that renders all data unrecoverable. This includes hard copy (paper) documents and any electronic media including computers, hard drives, magnetic tapes and USB storage devices.

Approved methods of disposal for hardcopy media include:

- Cross-cut shredding; and
- Incineration

Approved method of disposal for electronic media includes:

- Secure wipe program in accordance with industry-accepted standards for secure deletion; and
- Physically destroying the media until rendered unrecoverable.

BACKGROUND CHECK

Employees with direct access to, or control over credit cards, and/or credit card account information are considered to hold Sensitive Positions and are subject to background checks prior to the hire, transfer, reclassification, promotion or reassignment of individuals into sensitive positions, in accordance with CSU HR Coded Memo 2005-10 and/or its successor policy.

The only exception to this policy is for temporary cash handling activities (e.g., parking attendants, ticket sellers) which may not warrant background checks. Instead, mitigating supervisory review controls should be employed in such instances.

SERVICE PROVIDER

Ultimate responsibility for University PCI compliance resides with CSUF, regardless of how specific responsibilities may be allocated between CSUF and a Third Party Service Provider (TPSP). Specific guidelines for arrangements between the University and a TPSP include:

- University must perform thorough due diligence in selecting TPSPs that are appropriate and which third-party services are needed;
- University must perform a thorough risk assessment on its TPSP based on an industry-accepted methodology;
- TPSP must identify specific services being provided;
- TPSP may store, process, and transmit cardholder data on University's behalf, or may manage components of the University's cardholder data environment (CDE), such as routers, firewalls, databases, physical security, and/or servers;

- TPSP should be an integral part of the University's cardholder data environment (CDE) and will impact University's PCI DSS compliance, as well as the security of the CDE.

- TPSP shall have been certified and accredited by PCI SSC Council. List of such service providers can be found in APPENDIX A.

- TPSP must provide to the University documentation or evidence (e.g., SAQ, ROC or AOC) to ensure that service provider meets the intent of PCI DSS requirements. Such evidence or documentation should include:

    - Date of compliance assessment ;

    - System components, services, and environments that were included in the third-party PCI DSS assessment ; and

    - System components and services that were excluded from the PCI DSS assessment, as applicable to the service(s) provided.

- University must understand how the services provided by TPSPs correspond to the applicable PCI DSS requirements to assist in determining the potential security impact of utilizing TPSPs on the University's cardholder data environment.

- University shall include a contractual provision with the TPSPs that includes an acknowledgement that the TPSPs are responsible for the security of CHD the service provider possesses or otherwise stores, processes, transmits on behalf of University, or to the extent that they could impact the security of the University's cardholder data environment.

- University should include contractual provision with TPSPs that enable and require appropriate evidence sharing, including but not limited to:

    - PCI Attestation of Compliance, annually; or

    - ASV Scan Report Attestation of Scan Compliance (AOSC), annually; or

    - Report on Compliance (ROC), annually. It is possible that a TPSP may choose not to share certain aspects or any portion of its ROC if sensitive information is included or where releasing the document may compromise confidentiality; to avoid situations where the TPSP is not obligated to facilitate the evidence-sharing process.

- TPSP does not relieve the University of its own PCI DSS compliance responsibility, or exempt the University from accountability and obligation for ensuring that it's cardholder data (CHD), secured authenticated data (SAD), and CDE are secure.

- TPSP shall provide University electronic reports of daily transaction that may include: the last 4 digit of credit card number, tokens, or other form of codes that are no reflection of full credit card number on them.

- In the event of suspected system or data breaches, TPSP shall notify the University's ISO immediately. The University ISO must then file a security incident response per DR-10-Fullerton-Incident-Response-Protocol and ICSUAM section 8075.0, Information Security Policy. ISO must notify the Senior Director of System wide Information Security Management, CIO and the President who must notify the Chancellor, the CIO must notify the Assistant Vice Chancellor for Information Technology Services.

AUDIT AND ASSESSOR PROCESS

PCI Information Security Assessor (ISA) responsibilities include, but are not limited to, the following:

- Validate scope of the assessment
- Conduct PCI Data Security Standard assessments
- Verify all technical information given by stakeholders
- Use independent judgment to confirm requirements have been met
- Provide support and guidance during the compliance process
- Be onsite for the duration of any relevant assessment procedure
- Review the work product that supports the assessment procedures
- Adhere to the PCI DSS Requirements and Security Assessment Procedures
- Select representative samples of business facilities and system components where sampling is employed
- Evaluate compensating controls
- Produce final Attestation of Compliance report
- Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user;
- Audit all individual access to cardholder data;
- Audit all actions taken by any individual with root or administrative privileges (PCI DSS Requirement 10.2.2);

- Audit access to audit trails (PCI DSS Requirement 10.2.3);
- Audit invalid logical access attempts. (PCI DSS Requirement 10.2.4);
- Audit use of identification and authentication mechanisms. (PCI DSS Requirement 10.2.5); and
- Regularly test networks for exposed vulnerabilities and the continuous monitoring of security indicators, quarterly;
- Perform internal and external penetration testing of CDE, annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade or a sub-network or web server added to the environment). These penetration tests must include the following:
    - Network-layer penetration tests.
    - Application-layer penetration tests.

SECURITY AWARENESS PROGRAM

One of the biggest risks to information security is often not a weakness in the technology control environment. Rather it is the action or inaction by employees and other personnel that can lead to security incidents. It is therefore vital that the University has a security awareness program in place to ensure employees are aware of the importance of protecting sensitive information, what they should do to handle information securely, and the risks of mishandling information. Employees' understanding of the University and personal consequences of mishandling sensitive information is crucial to campus success.

Training objectives are to:

- Provide information on the University policy;
- Provide a fundamental understanding of the Payment Card Industry;
- Understand the intent of the PCI DSS requirements;
- Gain awareness of CHD security requirements for different payment environments, including:
    - Card present
    - Card-not-present
    - Phone
    - Mail
    - Fax

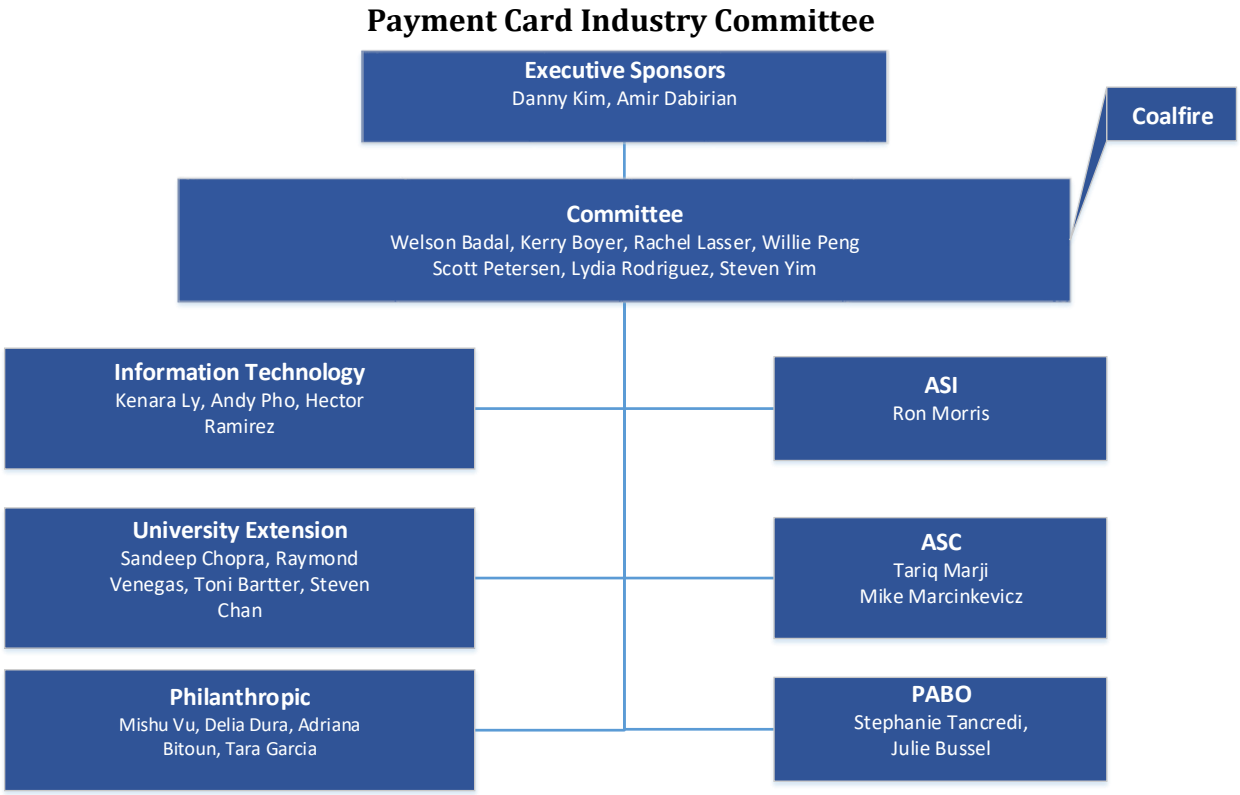
- Online (ecommerce)

- Understand the impact of unauthorized access;
- Avoid malicious software-viruses, spyware, adware, etc.;
- Secure browsing practices;
- Show how to report a potential security incident and who to report it to;
- Understand the significance of securing cardholder data;
- Gain understanding of the importance of strong passwords and password controls;
- Secure use of social media; and
- Protect against social engineering attach: in person - physical access; phone – caller ID spoofing; email – phishing, spear phishing; and, instant messaging

Beginning in Fall 2016, all personnel and future new hires will be required to undergo a one-time PCI Security Awareness training. Additional PCI training will be required of all specialized personnel with direct access to, or control over credit cards, and/or credit card account information, at least annually.

Individual acknowledgement will be required to ensure that specialized personnel have completed the training read and understood the University security policy and procedure.

APPENDIX A



PAYMENT CARD INDUSTRY COMPLIANCE COUNCIL (PCICC)

- University Controller
- Auxiliary Information System Officer
- Internal Security Assessor
- Auxiliary Financial Managers
- Information System Officer

REFERENCES AND RELATED DOCUMENTATION

Integrated CSU Administrative Manual (ICSUAM), Section 3102.05 Debit/Credit Card Payment Policy
http://www.calstate.edu/icsuam/sections.shtml

Integrated CSU Administrative Manual (ICSUAM), Section 3101.02 Campus Administration of Systemwide Cash Management

http://www.calstate.edu/icsuam/sections.shtml

PCI Security Standards Council

https://www.pcisecuritystandards.org/

ICSUAM section 8075.0, Information Security Policy

http://www.calstate.edu/icsuam/documents/Section8000.pdf

CSUF Cash Management Policy

http://finance.fullerton.edu/documents/controller/accounting/CSUFCashManagementPolicy.pdf

CSUF Merchant ID Request

https://finance.fullerton.edu/controller/MID.asp ***(Coming Soon)***

CSUF eMarket Site

http://finance.fullerton.edu/controller/eMarket.asp

HR Memo 2005-10

http://www.calstate.edu/audit/audit_reports/academicpersonnel/2011/1160aphum.pdf

List of TPSPs certified and accredited by PCI SSC Council

EMV VAR Service Providers
https://www.pcisecuritystandards.org/assessors_and_solutions/emv_var_service_providers

List Validated Payment Applications
https://www.pcisecuritystandards.org/assessors_and_solutions/payment_applications?agree=true

Approved PTS Devices
https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices

PCI Point-to-Point Encryption (P2PE) Solution
https://www.pcisecuritystandards.org/assessors_and_solutions/point_to_point_encryption_solutions

APPENDIX B

GLOSSARY

TERM	DEFINITION
Account Data	Account data consists of cardholder data and/or sensitive authentication data.
Account Number	See *Primary Account Number (PAN).*
Acquirer	Also referred to as "merchant bank," "acquiring bank," or "acquiring financial institution". Entity, typically a financial institution that processes payment card transactions for merchants and is defined by a payment brand as an acquirer. Acquirers are subject to payment brand rules and procedures regarding merchant compliance. See also *Payment Processor.*
Anti-Virus	Program or software capable of detecting, removing, and protecting against various forms of malicious software (also called "malware") including viruses, worms, Trojans or Trojan horses, spyware, adware, and rootkits.
AOC	Acronym for "attestation of compliance." The AOC is a form for merchants and service providers to attest to the results of a PCI DSS assessment, as documented in the Self-Assessment Questionnaire or Report on Compliance.
Application	Includes all purchased and custom software programs or groups of programs, including both internal and external (for example, web) applications.
ASV	Acronym for "Approved Scanning Vendor." Company approved by the PCI SSC to conduct external vulnerability scanning services.
Audit Log	Also referred to as "audit trail." Chronological record of system activities. Provides an independently verifiable trail sufficient to permit reconstruction, review, and examination of sequence of environments and activities surrounding or leading to operation, procedure, or event in a transaction from inception to final results.
Audit Trail	See *Audit Log.*
Authentication	Process of verifying identity of an individual, device, or process. Authentication typically occurs through the use of one or more authentication factors such as: a. Something you know, such as a password or passphrase b. Something you have, such as a token device or smart card c. Something you are, such as a biometric
Authentication Credentials	Combination of the user ID or account ID plus the authentication factor(s) used to authenticate an individual, device, or process

TERM	DEFINITION
Authorization	In the context of access control, authorization is the granting of access or other rights to a user, program, or process. Authorization defines what an individual or program can do after successful authentication. In the context of a payment card transaction, authorization occurs when a merchant receives transaction approval after the acquirer validates the transaction with the issuer/processor.
Backup	Duplicate copy of data made for archiving purposes or for protecting against damage or loss.
BAU	An acronym for "business as usual." BAU is an organization's normal daily business operations.
BEQ	Acronym for Business Environmental Questionnaire that merchant must first submit prior to acquiring merchant ID
Card Skimmer	A physical device, often attached to a legitimate card-reading device, designed to illegitimately capture and/or store the information from a payment card.
Card Verification Code or Value	Also known as Card Validation Code or Value, or Card Security Code. Refers to either: (1) magnetic or (2) printed security features. 1. Data element on a card's magnetic stripe that uses secure cryptographic processes to protect data integrity on the stripe, and reveals any alteration or counterfeiting. Referred to as CAV, CVC, CVV, or CSC depending on payment card brand. The following list provides the terms for each card brand: a. CAV – Card Authentication Value (JCB payment cards) b. PAN CVC – Card Validation Code (MasterCard payment cards) c. CVV – Card Verification Value (Visa and Discover payment cards) d. CSC – Card Security Code (American Express) 2. For Discover, JCB, MasterCard, and Visa payment cards, the second type of card verification value or code is the rightmost three-digit value printed in the signature panel area on the back of the card. For American Express payment cards, the code is a four-digit unembossed number printed above the PAN on the face of the payment cards. The code is uniquely associated with each individual piece of plastic and ties the PAN to the plastic. The following list provides the terms for each card brand: a. CID – Card Identification Number (American Express and Discover payment cards) b. PAN CVC2 – Card Validation Code 2 (MasterCard payment cards) c. CVV2 – Card Verification Value 2 (Visa payment cards)

TERM	DEFINITION
Cardholder	Non-consumer or consumer customer to whom a payment card is issued to or any individual authorized to use the payment card.
Cardholder Data	At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code
CDE	Acronym for "cardholder data environment." The people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data.
Compromise	Also referred to as "data compromise," or "data breach." Intrusion into a computer system where unauthorized disclosure/theft, modification, or destruction of cardholder data is suspected.
Default Accounts	Login account predefined in a system, application, or device to permit initial access when system is first put into service. Additional default accounts may also be generated by the system as part of the installation process.
Default Password	Password on system administration, user, or service accounts predefined in a system, application, or device; usually associated with default account. Default accounts and passwords are published and well known, and therefore easily guessed
e-Commerce	The process of conducting payment transactions over a computer network, usually the Internet. In e-commerce, card-not-present, customers enter that cardholder data online.
e-Merchant	Merchant who uses e-commerce system to generate revenue
FTP	Acronym for "File Transfer Protocol." Network protocol used to transfer data from one computer to another through a public network such as the Internet. FTP is widely viewed as an insecure protocol because passwords and file contents are sent unprotected and in clear text. FTP can be implemented securely via SSH or other technology
Host	Main computer hardware on which computer software is resident.
Hosting Provider	Offers various services to merchants and other service providers. Services range from simple to complex; from shared space on a server to a whole range of "shopping cart" options; from payment applications to connections to payment gateways and processors; and for hosting dedicated to just one customer per server. A hosting provider may be a shared hosting provider, who hosts multiple entities on a single server.

TERM	DEFINITION
Information Security	Protection of information to ensure confidentiality, integrity, and availability.
Information System	Discrete set of structured data resources organized for collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
IP Address	Also referred to as “internet protocol address.” Numeric code that uniquely identifies a particular computer (host) on the Internet.
LAN	Acronym for “local area network.” A group of computers and/or other devices that share a common communications line, often in a building or group of buildings.
Mainframe	Computers that are designed to handle very large volumes of data input and output and emphasize throughput computing. Mainframes are capable of running multiple operating systems, making it appear like it is operating as multiple computers. Many legacy systems have a mainframe design
Malicious Software / Malware	Software or firmware designed to infiltrate or damage a computer system without the owner's knowledge or consent, with the intent of compromising the confidentiality, integrity, or availability of the owner’s data, applications, or operating system. Such software typically enters a network during many business
Masking	In the context of PCI DSS, it is a method of concealing a segment of data when displayed or printed. Masking is used when there is no business requirement to view the entire PAN. Masking relates to protection of PAN when displayed or printed.
Merchant	For the purposes of the PCI DSS, a merchant is defined as any entity that accepts payment cards bearing the logos of any of the four members of PCI SSC (American Express, Discover, MasterCard or Visa) as payment for goods and/or services.
MID	Merchant ID, required to establish new payment processing
MO/TO	Acronym for “Mail
Network	Two or more computers connected together via physical or wireless means.
PAN	Acronym for “primary account number” and also referred to as “account number.” Unique payment card number (typically for credit or debit cards) that identifies the issuer and the particular cardholder account.
Password / Passphrase	A string of characters that serve as an authenticator of the user.

TERM	DEFINITION
Payment Application	In the context of PA-DSS, a software application that stores, processes, or transmits cardholder data as part of authorization or settlement, where the payment application is sold, distributed, or licensed to third parties
Payment Cards	For purposes of PCI DSS, any payment card/device that bears the logo of the founding members of PCI SSC, which are American Express, Discover Financial Services, JCB International, MasterCard Worldwide, or Visa, Inc.
Payment Processor	Sometimes referred to as "payment gateway" or "payment service provider (PSP)". Entity engaged by a merchant or other entity to handle payment card transactions on their behalf. While payment processors typically provide acquiring services, payment processors are not considered acquirers unless defined as such by a payment card brand.
PCI	Acronym for "Payment Card Industry."
PCICC	Acronym for "Payment Card Industry Compliance Committee." Consists of campus specialized personnel from division of Information Technology, Administration & Finance, ASC, ASI & Philanthropic.
PCI DSS	Acronym for "Payment Card Industry Data Security Standard."
PIN	Acronym for "personal identification number." Secret numeric password known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN the user provided matches the PIN in the system. Typical PINs are used for automated teller machines for cash advance transactions. Another type of PIN is one used in EMV chip cards where the PIN replaces the cardholder's signature.
POI	Acronym for "Point of Interaction," the initial point where data is read from a card. An electronic transaction