PAYMENT CARD POLICY

Payment Card Industry
Data Security Standard
(PCI DSS Version 4.0)

Contents

Purpose

This document and additional supporting documents represent Pepperdine University's policy/procedure suite to reduce the chance of loss/disclosure of sensitive customer information including payment card data. Failure to protect customer information may result in financial loss for customers, suspension of payment card processing privileges, and fines imposed on and damage to the reputation of the unit and the organization.

The Payment Card Policy establishes responsibility and authority for securing payment card account information at Pepperdine. The policy requires internal controls, testing, and training for compliance. The Payment Card Industry Data Security Standard (PCI DSS) is a mandated set of requirements agreed upon by the six major credit card companies: VISA, MasterCard, Discover, American Express, JCB, and UnionPay. These security requirements apply to all transactions surrounding the payment card industry and the merchants/organizations that accept credit and debit cards as forms of payment. Further details about PCI can be found on the PCI Security Standards Council (PCI SSC) website (https://www.pcisecuritystandards.org).

PCI DSS

The PCI DSS is a mandated set of technical and administrative requirements agreed upon by the six major credit card brands, and now maintained by the PCI SSC. These security requirements apply to all people, processes, and technologies that process, transmit, or store payment cardholder data (CHD), or that interact with payment card data or affect its security.

In order to accept payment cards, Pepperdine must maintain compliance with the PCI DSS at all times. Merchants must also assess/attest compliance status annually and, if found to be non-compliant at any time, must be actively working toward compliance in accordance with methodology and conditions set by their merchant services provider(s). Pepperdine University's Payment Card Policy and additional supporting documents provide the requirements for processing, transmitting, storage, and disposal of payment card data. This is done to reduce the organizational risk associated with the acceptance of card payments by individual departments and to ensure proper internal control and compliance with the PCI DSS.

Scope/Applicability

The Pepperdine University Payment Card Policy applies to all faculty, staff, students, organizations, third-party vendors, individuals, systems, and networks involved with payment card handling. This includes transmission, storage, and/or processing of payment card data, in any form (electronic or paper), on behalf of Pepperdine.

Authority

Pepperdine University policies fall within a greater hierarchy of laws, statutes, and regulations. The Board of Regents has been authorized by the State to govern Pepperdine University. The Board of Regents has delegated the authority to manage Pepperdine University PCI DSS to Jonathon See-Chief Information Officer, and Greg Ramirez-Chief Financial Officer. As a part of that management, the Chief Information Officer and Chief Financial Officer will direct the development and implementation of Pepperdine's policies and procedures.

Policy

It is the policy of Pepperdine University to allow acceptance of payment cards as a form of payment for goods and services upon written approval from the Pepperdine PCI Committee. Pepperdine requires all departments that accept payment cards to do so only in compliance with the PCI DSS and in accordance with this policy document, the Pepperdine payment card procedures, and other supporting documents.

All entities of Pepperdine that receive or expect to receive payments electronically must comply with the guidelines and procedures issued by the Pepperdine PCI Committee. All entities who wish to take payments via payment cards must be approved by the Pepperdine PCI Committee.

Departments must accept only payment cards authorized by Pepperdine's PCI Committee and agree to operate in accordance with the contract(s) Pepperdine University holds with its merchant services banking partners. This is to ensure that all transactions are in compliance with PCI DSS requirements, federal regulations, Nacha rules, service provider contracts, and Pepperdine University policies regarding security and privacy as they pertain to electronic transactions.

Departments must document and confirm the accuracy of their cardholder data environments (CDE) at least annually, and after any significant change. This documentation must cover all service providers, software, processing equipment, connections, and dataflows, and it must also ensure that an accurate inventory is in place.

Payment card data must be managed appropriately by implementing data retention and disposal policies, procedures, and processes that include at least the following for all payment card data storage:

- Limiting cardholder data storage amount and retention time to that which is required for legal, regulatory, and/or business reasons.
    - Documenting within the Departmental Payment Card Procedures the reason for and duration of any storage of cardholder data.
    - Documenting any temporary storage of sensitive authentication data (SAD) prior to authorization (storage of SAD after authorization is **never** permitted) such that only authorized personnel have access.
- Data that is not required to conduct business must not be retained in any format (paper or electronic).

- Processes for secure deletion of data when it is no longer needed, or the retention period is met.

- A quarterly process for identifying and securely deleting stored cardholder data that exceeds the defined retention.
- Physical access to data records is restricted to staff with a job-related need.

Cardholder data received via end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.) is never to be used to process a payment. Follow approved departmental procedures for the appropriate method of responding to the message, redirecting to an acceptable payment channel, and securely destroying the cardholder data.

All **processing equipment** must be approved by ISO and the Finance office. Exceptions to this policy must be reviewed and approved by the Pepperdine PCI Committee in advance of any equipment, software, or system procurement, and will require documentation of the reason(s) why the available central processing solutions will not meet customer service requirements.

All payments received must be directed into a Pepperdine **approved bank account**. The type and nature of the electronic transaction (e.g., ACH, credit/debit card, wire, etc.) will dictate where the transaction will be deposited.

Accounting entries to record the receipt of the payment will be linked directly into Pepperdine University central financial information system, whenever possible, to ensure timely recording of transactions and expedite the prompt reconciliation of general ledger and bank accounts.

Sanctions

Failure to meet the requirements outlined in this policy will result in suspension of the physical and, if appropriate, electronic payment capability for the affected merchant(s). In the event of a breach or a PCI violation the payment card brands may assess penalties to the organization's merchant services bank which will likely then be passed on to the organization. Any fines and assessments imposed will be the responsibility of the impacted merchant. A one-time penalty of up to $500,000 per card brand per breach can be assessed as well as on-going monthly penalties and/or categorization as a Level 1 merchant, which would likely require the organization to hire a Qualified Security Assessor (QSA) company annually to conduct a Report on Compliance (ROC).

Persons in violation of this policy are subject to sanctions, including loss of computer or network access privileges, disciplinary action, suspension, and termination of employment, as well as legal action. Some violations may constitute criminal offenses under local, state, or federal laws. Pepperdine University will carry out its responsibility to report such violations to the appropriate authorities.

Procedures and Other Supporting Documents

- Pepperdine University - Departmental Payment Card Procedures
- Pepperdine University - Payment Card Security Incident Response Plan

- Pepperdine University - Application for New Payment Card Merchants
- Pepperdine University - Annual Merchant Survey
- Pepperdine University - Payment Card Best Practices
- Pepperdine University - PCI PoS Terminal Requirements

Interpretations

The authority to interpret this document rests with the Information Security Office and the Pepperdine PCI Committee.

Glossary

Acquirer	See *Merchant Bank* and *Payment Processor*.
Antivirus Software	Software program that detects, removes, and protects against malicious software (also called "malware") including viruses, worms, Trojans or Trojan horses, spyware, adware, and rootkits. Also called "anti-malware software."
Application	Software program or group of programs that runs on a PC, smartphone, tablet, internal server, or web server.
Approved Scanning Vendor (ASV)	Company approved by the PCI Security Standards Council to conduct external vulnerability scanning services to identify common weaknesses in system configuration.
Authentication	Method for verifying the identity of a person, device, or process attempting to access a computer. To confirm the identity/user is valid, one or more of the following is provided: • A password or passphrase (something the user knows) • A token, smart card, or digital certificate unique to the user (something the user has) • A biometric identifier, such as a fingerprint (something the user is or does)
Authorization	In a payment card transaction, authorization occurs when a merchant receives transaction approval after the acquirer validates the transaction with the issuer/processor.
Bank Identification Number (BIN)	The first six digits (or more) of a payment card number that identifies the financial institution that issued the payment card to the cardholder.
Business Need-to-Know	The principle that access to systems or data is granted by a user's business need—only what is necessary for a user's job function.
Card Data / Customer Card Data	At a minimum, card data includes the primary account number (PAN) and may also include cardholder name and expiration date. The PAN is visible on the front of the card and encoded into the card's magnetic stripe and/or the embedded chip. Also referred to as cardholder data. See also *Sensitive Authentication Data* for additional data elements which may be part of a payment transaction, but which must not be stored after the transaction is authorized.
Chip	Also known as "EMV Chip." The microprocessor (or "chip") on a payment card used when processing transactions in accordance with the international specifications for EMV transactions.
Chip and PIN	A verification process where a consumer enters their PIN in an EMV Chip-enabled payment terminal when they purchase goods or services.
Chip and Signature	A verification process where a consumer uses their signature with an EMV Chip-enabled payment terminal when they purchase goods or services.
Credential	Information used to identify and authenticate a user for access to a system. For example, credentials are often the username and password. Credentials may include a fingerprint, retina scan, or a one-time number generated by a portable "token-generator." Security is stronger when access requires multiple credentials.

Cryptography	Cryptography is the method of securing data by making it unintelligible to a human or computer. Cryptography is only useful when the intended recipient can reassemble the data into a readable form using a method known only to the sender and receiver. See also *Encryption.*
Cyberattack	Any offensive action to break into a computer or system. Cyberattacks can range from installing spyware on a PC, breaking into a payment system to steal card data, or attempting to break critical infrastructure such as an electric power grid.
Data Breach	A data breach is an incident in which sensitive data may have potentially been viewed, stolen, or used by an unauthorized party. Data breaches may involve card data, personal health information (PHI), personally identifiable information (PII), trade secrets, or intellectual property, etc.
Default Password	A simple password that comes with new software or hardware. Default passwords (like "admin" or "password" or "123456") are easily guessed and usually are available via online search. They are intended as a placeholder and offer no real security—and must be changed to a stronger password after installing new software or hardware.
Data Security Essentials (DSE)	Data Security Essentials for Small Merchants is a set of educational resources and an evaluation tool to help merchants simplify their security and reduce risk. DSE is intended as an alternative approach to the PCI DSS Self-Assessment Questionnaires (SAQs) for those merchants designated as eligible by the payment brands and their acquirers (merchant banks).
Electronic Cash Register (ECR)	A device that registers and calculates transactions and may print out receipts but does not accept customer card payments. Also called a "till."
Encryption	Process of using cryptography to mathematically convert information into a form unusable except to holders of a specific digital key. Use of encryption protects information by devaluing it to criminals. See also *Cryptography*.
Firewall	Hardware and/or software that protects network resources from unauthorized access. A firewall permits or denies communication between computers or networks with different security levels based upon a set of rules and other criteria.
Forensic Investigator	PCI Forensic Investigators (PFIs) are companies approved by the PCI Council to help determine when and how a card data breach occurred. They perform investigations within the financial industry using proven investigative methodologies and tools. They also work with law enforcement to support stakeholders with any resulting criminal investigations.
Hacker	A person or organization that attempts to circumvent security measures of computer systems to gain control and access. Usually this is done in an effort to steal card data.
Hosting Provider	Offers various services to merchants and other service providers, where their customers' data is "hosted" or resident on the provider's servers. Typical services include shared space for multiple merchants on a server, providing a dedicated server for one merchant, or web apps such as a website with "shopping cart" options.
Integrated Payment Terminal	A payment terminal and electronic cash register in one device that takes payments, registers and calculates transactions, and prints receipts.

Integrator/Reseller	An integrator/reseller is a company that merchants work with to help set up their payment system. This may include installation, configuration, and support. These companies may also sell payment devices or applications as part of their service. See also *Qualified Integrator Reseller (QIR)*.
Log	A file that is created automatically when certain predefined (often security-related) events occur within a computer system or network. Log data includes date/time stamp, description of the event, and information unique to that event. These files are useful for troubleshooting technical issues or a data breach investigation. Also called an "audit log" or "audit trail."
Malware	Malicious software designed to infiltrate a computer system with the intent of stealing data, or damaging applications or the operating system. Such software typically enters a network during many business-approved activities such as via email or browsing websites. Malware examples include viruses, worms, Trojans (or Trojan horses), spyware, adware, and rootkits.
Merchant Bank	A bank or financial institution that processes credit and/or debit card payments on behalf of merchants. Also called an "acquirer," "acquiring bank," "card processor," or "payment processor." See also *Payment Processor*.
Mobile Device	Devices such as smart phones and tablets that are small, portable, and can connect to computer networks wirelessly.
Mobile Payment Acceptance	Using a mobile device to accept and process payment transactions. The mobile device is usually paired with a commercially available card-reader accessory.
Multi-factor Authentication	Method of authenticating a user when two or more factors are verified. These factors include something the user has (such as a smart card or dongle), something the user knows (such as a password, passphrase, or PIN) or something the user is or does (such as fingerprints, other forms of biometrics, etc.).
Network	Two or more computers connected via physical or wireless means.
Operating System	Software on a computer system that provides overall management and coordination of computer activities. Examples include Microsoft Windows, Apple OSX, iOS, Android, Linux, and UNIX.
P2PE	Acronym for the PCI Security Standards Council's Point to Point-Encryption standard. See details at www.pcisecuritystandards.org.
Password	A word, phrase, or string of characters used to authenticate a user. When combined with the username, the password is intended to prove the identity of the user for access to computer resources.
Patch	Update to existing software that adds functionality or corrects a defect (or "bug").
Payment Application	Related to PCI Secure Software Standard (see SSC, below), a software application that stores, processes, or transmits cardholder data as part of authorization or settlement of payment transactions.
Payment Application Vendor	Vendor that sells applications that store, process, and/or transmit card data during payment transactions.

Payment Middleware	A general term for software that connects two or more, perhaps unrelated, payment applications together. For example, it may pass card data between an application on a payment terminal and other merchant systems that send card data to a processor.
Payment Processor	Entity engaged by merchants to handle payment card transactions on their behalf. While payment processors typically provide acquiring services, payment processors are not considered acquirers (merchant banks) unless defined as such by a payment card brand. Also called a "payment gateway" or "payment service provider" (PSP). See also *Merchant Bank.*
Payment System	Encompasses the entire process for accepting card payments in a merchant retail location (including stores/shops and ecommerce storefronts) and may include a payment terminal, an electronic cash register, other devices or systems connected to the payment terminal (for example, Wi-Fi for connectivity or a PC used for inventory), servers with ecommerce components such as payment pages, and the connections out to a merchant bank.
Payment System Vendor	A vendor who sells, licenses, or distributes a complete payment solution to a merchant. The solution encompasses the hardware and software needed to handle payments within the store and provides a method to connect to a payment processor.
Payment Terminal	Hardware device used to accept customer card payments via swipe, dip, insert, or tap. Also called "point-of-sale (POS) terminal," "credit card machine," or "PDQ terminal."
PCI	Acronym for Payment Card Industry.
PCI DSS	Acronym for the PCI Council's "Payment Card Industry Data Security Standard." See details at www.pcisecuritystandards.org.
PCI DSS Compliant	Meeting all applicable requirements of the current PCI DSS, on a continuous basis via a business-as-usual approach. Compliance is assessed and validated at a single point in time; however, it is up to each merchant to continuously follow the requirements in order to provide strong security. Merchant banks and/or the payment brands may have requirements for formal annual validation of PCI DSS compliance.
PCI DSS Validated	Providing proof that all applicable PCI DSS requirements are met at a single point in time. Depending on specific merchant bank and/or payment brand requirements, validation can be achieved through the applicable PCI DSS Self-Assessment Questionnaire or by a Report on Compliance resulting from an onsite assessment.
PCI Validated Payment Application	Software application that has been validated per the PCI Secure Software Standard (SSC) and is listed on the PCI Council website.
PCI-Approved Payment Terminal	Payment terminal that has been approved per the PCI PIN Transaction Security (PTS) standard and is listed on the PCI Council website.
PCI-Listed Point-to-Point Encryption Solution	Encryption solution that has been validated per the PCI Point-to-Point-Encryption (P2PE) standard and is listed on the PCI Council website.
PED	Acronym for "PIN entry device." Keypad into which the customer enters their PIN. Also called a "PIN pad."

PIN	Acronym for "personal identification number." A unique number known only to the user and a system to authenticate the user to the system. Typical PINs are used for automated teller machines for cash advance transactions, or for EMV chip cards to replace a cardholder's signature. PINs help determine whether a cardholder is authorized to use the card and to prevent its unauthorized use if the card is stolen.
Primary account number (PAN)	Unique number for credit and debit cards that identifies the cardholder account.
Privilege Abuse	Using computer system access privileges in an abusive manner. Examples include a system administrator accessing card data for malicious purposes, or someone stealing and using an administrator's elevated access privileges for malicious purposes.
PTS	Acronym for the PCI Council's PIN Transaction Security standard. PTS is a set of modular evaluation requirements for PIN acceptance point-of-interaction (POI) terminals. See details at www.pcisecuritystandards.org.
QIR	Acronym for "Qualified Integrator or Reseller." QIRs are integrators and resellers specially trained by the PCI Security Standards Council to address critical security controls when installing merchant payment systems. See details at *www.pcisecuritystandards.org*.
Qualified Security Assessor\ Company (QSAC)	A company approved by the PCI Security Standards Council to validate an entity's adherence to PCI DSS requirements.
Recurring Payment	A billing method where merchants bill their customers repeatedly over time, such as for monthly memberships or subscriptions. A secure way to do this is for the acquirer/processor to tokenize the card data, which ensures its protection and relieves the merchant from this responsibility.
Remote Access	Access to a computer network from a location outside of that network. Remote access connections can originate either from inside the company's own network or from a remote location. An example of technology for remote access is a virtual private network (VPN). Remote access can be either internal (e.g. IT support) or external (e.g., service providers, third-party agents, integrators/resellers).
Reseller / Integrator	An entity that sells and/or integrates payment applications but does not develop them.
Router	Hardware or software that connects two or more internal or external computer networks to "route" or guide data through a network, and to ensure the data flows properly between those networks. The router can also create more security by permitting only approved traffic and denying unapproved traffic.
Secure Card Reader (SCR)	A PTS-approved device that attaches to a mobile phone or tablet for securely accepting payment cards. PCI PTS-approved SCRs protect and encrypt the card data via SRED. See also *SRED*.
Security Code	A three- or four-digit value printed onto the front or back signature panel of a payment card. This code is uniquely associated with an individual card and is used as an additional check to ensure that the card is in possession of the legitimate cardholder, typically during a card-not-present transaction. Also referred to as card security code.
Self-Assessment Questionnaire (SAQ)	A questionnaire covering a set of PCI DSS requirements that is completed by the organization itself to confirm it is meeting those requirements.

Sensitive Authentication Data	Security-related information used to authenticate cardholders and/or authorize payment card transactions, stored on the card's magnetic stripe or chip.
Service Provider	A business entity that provides various services to merchants. Typically, these entities store, process, or transmit card data on behalf of another entity (such as a merchant) OR are managed service providers that provide managed firewalls, intrusion detection, hosting, and other IT-related services. Also called a "vendor."
Skimming	Stealing card data directly from the consumer's payment card or from the payment infrastructure at a merchant location such as with an unauthorized hand-held card reader or via modifications made to the merchant's payment terminal. Its purpose is to commit fraud, the threat is serious, and it can hit any merchant's environment.
Skimming Device	A physical device, often attached to a card-reading device, designed to illegally capture and/or store the information from a payment card. Also called a "card skimmer."
Small Merchant	A small merchant is typically an independently owned and operated business with a single location or a few locations, and with limited or no IT budget and often with no IT personnel. Whether a small merchant is required to validate PCI compliance is determined by the payment brand or acquirer (merchant bank).
SRED	An acronym for "Secure Reading and Exchange of Data." A set of PCI PTS requirements designed to protect and encrypt card data in payment terminals. A PCI Council-listed Point-to-Point Encryption (P2PE) solution must use a PTS-approved and listed payment terminal with SRED enabled and actively performing card data encryption.
Secure Software Standard (SSS)	A software security standard within the Software Security Framework (SSF) designed to provide to merchants validated payment applications and/or modules providing payment-related services that might reduce the scope of applicable PCI DSS requirements.
Stand-Alone Terminal	A payment terminal that does not rely on connection to any other device within the merchant environment and performs no other functions. The only requirement for it to operate is a connection to the processor through either an Internet connection or a telephone line. If the terminal requires connection to a computerized electronic cash register or is multi-function (like a mobile device), it is not a stand-alone terminal.
Strong Authentication	Used to verify the identity of a user or device to ensure the security of the system it protects. The term strong authentication often means with multifactor authentication (MFA).
Till	See *Electronic Cash Register*.
Tokenization	A process by which the primary account number (PAN) is replaced with an alternative value called a token. Tokens can be used in place of the original PAN to perform functions when the card is absent like voids, refunds, or recurring billing. Tokens also provide more security if stolen because they are unusable and thus have no value to a criminal.
Unencrypted Data	Any data that is readable without the need to decrypt it first. Also called "plaintext" and "clear-text" data.

Vendor	A business entity that supplies a merchant with a product or service needed for the course of business. Where services are offered, the vendor may be considered a service provider and may require access to physical locations or computer systems within the merchant environment that could affect the security of card data. See also *Service Provider*.
Virtual Payment Terminal	Web-browser-based access to an acquirer, processor or third-party service provider website to authorize payment card transactions. Unlike physical terminals, virtual payment terminals do not read data directly from a payment card. The merchant manually enters payment card data via the securely connected web browser. Because payment card transactions are entered manually, virtual payment terminals are typically used instead of physical terminals in merchant environments with low transaction volumes.
Virtual Private Network (VPN)	Software that creates a secure, private channel for exchanging data and conducting phone calls over the Internet.
Virus	Malware that replicates copies of itself into other software or data files on an "infected" computer. Upon replication, the virus may execute a malicious payload, such as deleting all data on the computer. A virus may lie dormant and execute its payload later, or it may never trigger a malicious action. A virus that replicates itself by resending itself as an e-mail attachment or as part of a network message is called a "worm."
Vulnerability	Flaw or weakness which, if abused, may result in an intentional or unintentional compromise of a system.
Vulnerability Scan	A software tool that detects and classifies potential weak points (vulnerabilities) on a computer or network. A quarterly external vulnerability scan per PCI DSS Requirement 11.2.2 must be performed by an Approved Scanning Vendor. Other vulnerability scans (such as internal scans and those performed after network changes) can be conducted by qualified staff in an organization's IT department or by a security service provider (such as an Approved Scanning Vendor). *See also Approved Scanning Vendor (ASV).*
Wi-Fi	Wireless network that connects computers without a physical connection to wires.
Wireless Payment Terminal	Payment terminal that connects to the Internet using any of various wireless technologies.