UNLV Payment Card Merchant Policy
Payment Card Handling Responsibilities and Procedures

Background

Colleges and universities have traditionally had open networks of information that foster the exchange of ideas and information. However, college and university networks have sometimes been invaded by hackers. This can result in security breaches that disclose customers' payment card information. To protect our customers' payment card information, the university's reputation, and to reduce the financial costs associated with a breach of payment card information, UNLV has instituted this Payment Card Merchant Policy.

Due to the recent increase in breaches and the resulting customer distrust in the use of payment cards as a secure option, the card associations, including Visa, MasterCard, American Express, JCB, and Discover, have formed the Payment Card Industry Security Standards Council (PCI SSC). The PCI SSC has developed the Payment Card Industry Data Security Standards (PCI DSS) to assure consumers that their brands and payment cards are reliable and secure. These standards include controls for handling and restricting access to payment card information, computer and Internet security, and reporting of a breach of payment card information. PCI DSS applies to all entities involved in payment card processing - including merchants, processors, financial institutions, and service providers, as well as all other entities that store, process, transmit, or affect the security of cardholder data. These standards are enforced by the card associations and adherence is required in order for a merchant to accept card payments.

A payment card merchant is a department or any other entity at the university that stores, processes, transmits, or affects the security of cardholder data. All merchants at the university are required to use the NSHE contracted merchant services provider to settle payment card transactions.

Additionally, web payment vendors are required to use a web payment gateway vendor approved by the university Controller's Office in consultation with the "NSHE contracted merchant services provider" and "NSHE contracted PCI approved vendor". The Controller's Office relies on the "NSHE contracted merchant services provider" and the "NSHE contracted PCI approved vendor" to ensure that web payment gateway vendors are PCI compliant.

All university merchants must complete a Self- Assessment Questionnaire (SAQ) annually. If applicable, vulnerability scans and/or penetration testing by our PCI approved vendor may be required.by our PCI approved vendor.

Purpose

This Policy defines the steps that payment card merchant account holders at UNLV must use to access and secure payment card data. It also establishes responsibility for all steps in the processing of payment card data, self-assessment of the merchant account, and remediation of non-compliant processes associated with storing, transmitting, processing, and affecting the security of payment card data.

All compliance reviews for merchant accounts will be coordinated by the Controller's Office. Payment card handling procedures may be subject to audit by internal audit or external audit. Departments not complying with approved safeguarding of processing equipment and cardholder's data, self-assessment procedures, trainings, and processing procedures may lose merchant privileges.

Compliance requirements for each merchant are determined based on the type and volume of payment card transactions. All business accepting payment cards will be required to complete an annual self-assessment questionnaire (SAQ). The Controller's Office will coordinate with the business units to ensure completion and filing of any required reports with the university's merchant services provider or bank.

Who Should Know This Policy

Any official or administrator with responsibilities for managing university payment card transactions and all employees involved with handling cardholder data must be aware of this policy. This includes program managers and systems managers.

To Whom This Policy Applies

This policy applies to all merchants at the university that accept payment cards via any channel. Specifically, it applies to merchants accepting payments via a payment card terminal as well as merchants processing or sending transactions over the Internet. Internet transactions include links on UNLV websites redirecting customers to another website, as well as use of Point-of-Sale software, or a third-party vendor to transmit, process, or store cardholder data.

Business units wishing to accept credit card payments must comply with the Payment Card Industry Data Security Standards (PCI-DSS). The standards established by the payment card industry are based on best practices in data security. Compliance with PCI standards protects the university's students, customers and employees.

General Responsibilities and Requirements

Responsibilities of the Controller's Office

- Administer the process of obtaining new merchant accounts
- Communicate the policy and PCI DSS to merchants
- Advise merchants wanting to accept payment cards as to their compliant options
- Process First Notice Rule Set to automate the accounting in the financial system
- Coordinate periodic reviews of existing merchants to include verification of procedures and computer scans as appropriate
- Coordinate annual completion of merchant SAQs and submission of university SAQ to the bank

Responsibilities of Department Payment Card Merchants

All merchants must comply with the requirements listed in the section below titled "General Responsibilities for all Departments utilizing Payment Card Merchant Accounts." These responsibilities include PCI DSS requirements and university requirements. In addition, merchants must refer to the specific requirements listed in the "Payment Card Merchant Policy for Terminal and Internet related processing" in this document.

General Responsibilities for All Departments utilizing Merchant Accounts

All Payment Card Transaction Types

- **Comply with applicable sections of the Payment Card Industry (PCI) Data Security Standards (DSS).** Comply with the applicable provisions of the current PCI DSS found on the following website. https://www.pcisecuritystandards.org/
- **New merchants or new purchases** - Approval by the Controller's Office before entering into any contract, purchase, acquisition, or replacement of equipment, software, Internet provider, or wireless device that processes payment card transactions.
- **Maintain a department information security policy –** Departments utilizing payment card merchant accounts must establish policies and procedures for physically and electronically safeguarding cardholder data. **(Please use the form titled "Responsibilities of Payment Card Handlers and Processors" (Appendix A) and make the necessary additions pertaining to your department's payment card processing arrangement.)** (PCI DSS 12)
- **Prevent unauthorized access to cardholder data and secure the data –** Establish procedures to prevent access to cardholder data in all forms including but not limited to the following: hard copy or media containing payment card information must be stored in a locked drawer or office; department should establish password protection on computers; visitor sign-in logs, escorts and other means must be used to restrict access to documents, servers, computers, and storage media.
- **Communicate policy to staff and obtain signatures** – Supervisors including Deans, fiscal officers, and systems managers must communicate this policy to their staff and maintain the **"Responsibilities of Payment Card Handlers and Processors" form** for all personnel involved in payment card transactions.
- **Restrict access based on a business need-to-know –** Access to physical or electronic cardholder data must be restricted to individuals whose job requires access.
- **Assign a unique ID to each person with computer access** – A unique ID must be assigned to each person with access to computers that are used to process payment card information. User names and passwords may not be shared.
- **Transmitting cardholder data by e-mail, chat or eFax is strictly prohibited** – Never send unprotected Primary Account Number (PAN) by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.)
- **Electronically storing the CVV/CVV2 validation code, or PIN number is prohibited -** Do not store the three- or four-digit CVV or CVV2 validation code, or the PIN, (personal identification number).
- **Segregation of duties** - Establish appropriate segregation of duties between personnel processing transactions, issuing refunds to custody of assets, record keeping and those assigned to the reconciliation function.
- **Mask the payment card number -** Terminals and computers must mask everything but the first 6 digits and the last 4 digits of the PAN.

Specific Procedures for On-going Operations

All Payment Card Transaction Types

- Do not disclose or acquire any cardholder data without the cardholder's consent.
- Keep all cardholder data and sensitive authentication data secure and confidential and limit access to only those employees who require access to do their job.
- Cardholder data cannot be stored in any fashion on UNLV computers, networks or related media.
- Wireless networks cannot be used in the cardholder data environment.
- Cardholder data must never be transmitted via email and departments are prohibited from soliciting cardholder data via e-mail.
- Cardholder data that is inadvertently received by e-mail should be deleted immediately and may not be used for processing payments.
- Payment card authorization forms must not contain references to an e-mail address
- Payment card authorization forms must not contain a FAX number that refers to an unsecured FAX machine.
- Payment card authorization forms must clearly show the following warning, "Please do NOT e-mail this authorization form. E-mail is NOT a secure way of transmitting your card information."
- All documentation containing cardholder data must be destroyed in a manner that will render them unreadable (crosscut shredding or third-party shred bin) after their useful life (180 days) has expired. All other departmental deposit and accounting records must be maintained for a period of seven (7) years.
- A report of activity (by day and in total) is to be generated each month. This report should include your merchant name and number, the daily totals by batch, sales distribution, and total for the month.
- Reconcile daily activity to merchant statements at least monthly to ensure credit is received for all processed transactions. Verify amount to finance deposit postings. Documentation that a reconciliation was done should be retained by the Department.
- All business units which accept payment cards will be required to complete an annual self-assessment questionnaire (SAQ).
- Each department that processes payment card transactions must have written procedures specific to that organization. The procedures must include, but are not limited to, the following:
    - Segregation of duties
    - Reconciliation procedures – daily and monthly
    - Physical security
    - Disposal
    - Instructions for processing transactions through all accepted payment channels
- Departmental procedures should be reviewed, signed and dated by the Department Manager, Business Manager and Dean/Director on an annual basis and submitted to the Controller's Office along with other required PCI compliance documentation.
- For assistance in developing departmental procedures, please contact the Controller's Office – PCI Compliance Team at pci@unlv.edu.

Over the Counter Transactions

- Verify signature of cardholder at the time of the transaction.
- Obtain the signature of the cardholder on the receipt and provide the duplicate copy to the cardholder.
- Be sure only the last four digits of the card number are printed on the receipt.
- Store the departmental copy of the receipt safely until it is needed for end of day balancing.
- Keep all receipts for each day together. Compare them to daily totals and then group them with the daily batch settlement tape for storage/reference purposes.
- Record the batch total and batch number for each day in the monthly summary report.
- If for any reason the terminal does not work, use the standardized payment form and provide the bottom portion as the cardholder's receipt. Include a description of the transaction, the transaction date, and the dollar amount on the portion signed by cardholder and give them a copy for their records. Hand enter when the terminal is running again. Keep the original copy of the form and destroy validation code immediately after processing in a manner that will render them unreadable (crosscut shredding or third-party shred bin).
- Log and inspect terminal or card swipe mechanism to ensure it has not been tampered with and is working properly.
    - Daily for publicly accessible readers or devices used infrequently, weekly for supervised readers that may have exposure to public or non-PCI staff, and monthly for those located in a secure office.
- Terminal or card swipe mechanism must be stored securely overnight.

Mail-in, FAX and Phone Orders

- Maintain a payment listing for balancing and accounting purposes. This listing should not contain the cardholder data –the last four digits of the card number may be listed.
- FAX machines must be a secure analog standalone machine (does not include eFax) and should be located in a nonpublic area where access is limited to accountable, dependable and trustworthy staff.
- Documents with the card number and other cardholder data should be processed promptly and then safely stored if needed for balancing the day's transactions. Cardholder's three (3) or four (4) digit validation code must be destroyed immediately after processing in a manner that will render them unreadable (crosscut shredding or third-party shred bin).
- Documents with card number and other cardholder data should be destroyed after balancing the day's transactions or after the transaction is submitted.
- Keep all receipts for each day together. Compare them to daily totals and then group them with the daily batch settlement tape for storage/reference purposes.
- Record the batch total and batch number for each day in the monthly summary report.

Internet (E-Commerce) Orders

- All payment card transactions must be processed by a PCI DSS compliant third-party provider and the account must be opened by the Controller's Office with approval by Purchasing and "NSHE contracted PCI approved vendor."
- No cardholder data can be stored on UNLV servers or networks.

- Review and comply with UNLV's "Computer Security Policy" and "Password Policy" available on the IT website. https://www.it.unlv.edu/policies
- Periodic network vulnerability scans will be conducted and the department is responsible for timely remedy of deficiencies.
- Documented verification that systems and technology used meet all required PCI DSS security protocols should be kept on file in the department.
- This verification will be obtained in coordination with the Controller's Office by contacting the PCI Compliance Team at pci@unlv.edu.
- Changes to electronic processing systems (departmental software, website, etc.) must be communicated to Controller's Office and confirmed to maintain compliance with PCI DSS before changes are made.

Chargebacks

- A chargeback occurs when the Customer or the Customer's bank challenges all or part of a payment card transaction. An adjustment may be applied to your account.
- A chargeback is a reduction of your revenue. The Department will submit the required documentation in response to the request.
- You should not issue a credit after you have received notification of a dispute because the Customer's bank may have applied a conditional credit to the Customer's account. You may not be able to recover a credit after a chargeback has been received if you issue a credit in these circumstances; in fact, you may be responsible for the credit and chargeback.
- Chargeback forms should be maintained in the department and a note made in the customer's file of the chargeback and the circumstances.
- Departments should periodically review their chargebacks to see if there are internal policies that need to be changed so that fewer transactions are disputed.

First Notice Rule Set

- A First Notice Rule Set contains an ad hoc bank transaction template with the department's accounting information linking to a conditional rule that searches the bank account specified in the conditions.
- When the conditions are met (i.e., search addenda for merchant account number on the UNLV General bank account) from the rules within each rule set, Workday creates an ad hoc bank transaction from the template created for the first-notice rule set.
- Workday finds bank statement items that don't have an accounting entry reconciled. With the First Notice Rule Set, a department's accounting and the banking is automatically reconciled within the financial system.
- First Notice Rule Sets do not substitute or eliminate the business units need to perform their reconciliation process and to ensure all transactions have been received.

APPENDIX A
Responsibilities of
Payment Card Handlers and Processors

As an individual person involved in the handling of cardholder data, I agree to abide by the provisions in this document. If I need further clarification, I will refer to UNLV Payment Card Merchant Policy.

I will NOT do the following:

1. Acquire or disclose any cardholder's data without the cardholder's consent including but not limited to the full or partial sixteen (16) digit primary account number, three (3) or four (4) digit validation code (usually on the back of payment cards), or PINs (personal identification numbers).
2. Store any documents that have cardholder's three (3) or four (4) digit validation code.
3. Transmit cardholder's data by e-mail, chat or eFax.
4. Electronically store cardholder data on a university computer file or server.
5. Share a computer login or password if I have access to a computer used to process cardholder data.

I will DO the following:

1. Maintain up-to-date departmental procedures reviewed, signed and dated by the Department Manager, Business Manager and Dean/Director on an annual basis.
2. At time of employment, agree to complete a background check within the limits of local law.
3. Change a vendor-supplied or default password if I have access to a computer with cardholder data.
4. Comply with university policies regarding the implementation and maintenance of passwords at all times, including, but not limited to the use of passwords on all equipment used in payment processing.
5. Escort and supervise all visitors including UNLV personnel in areas where cardholder data is maintained.
6. Store all physical documents or storage media containing cardholder data in a locked drawer, locked file cabinet, or locked office.
7. Destroy all documents containing cardholder data in a manner that will render them unreadable (crosscut shredding or third-party shred bin).
8. Immediately report a payment card security incident to my supervisor and the PCI Compliance Team if I know or suspect payment card information has been exposed, stolen, or misused.
    a. Notification to Supervisor should be in writing.
    b. Notification to PCI Compliance Team should go through the data breach form. (This report must not disclose by FAX, chat or e-mail any cardholder data, three- or four-digit validation codes, or PIN numbers. It must include a department name and contact number.)

APPENDIX B
PCI DEFINITIONS AND LINKS

Account Data - Account data consists of cardholder data and/or sensitive authentication data. See Cardholder Data and 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. **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:

- Something you know, such as a password or passphrase
- Something you have, such as a token device or smart card
- Something you are, such as a biometric

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.
Bluetooth - Wireless protocol using short-range communications technology to facilitate transmission of data over short distances.
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-stripe data, or (2) printed security features. 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:

- CAV – Card Authentication Value (JCB payment cards)
- PAN CVC – Card Validation Code (MasterCard payment cards)
- CVV – Card Verification Value (Visa and Discover payment cards)
- CSC – Card Security Code (American Express)

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:

- CID – Card Identification Number (American Express and Discover payment cards)
- CAV2 – Card Authentication Value 2 (JCB payment cards)
- PAN CVC2 – Card Validation Code 2 (MasterCard payment cards)
- CVV2 – Card Verification Value 2 (Visa payment cards)

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
- Service code

See Sensitive Authentication Data for additional data elements that may be transmitted or processed (but not stored) as part of a payment transaction.
CDE - Acronym for "cardholder data environment." The people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data.
CIS - Acronym for "Center for Internet Security." Non-profit enterprise with mission to help organizations reduce the risk of business and e-commerce disruptions resulting from inadequate technical security controls.
Compensating Controls - Compensating controls may be considered when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints, but has sufficiently mitigated the risk associated with the requirement through implementation of other controls. Compensating controls must:

- Meet the intent and rigor of the original PCI DSS requirement;
- Provide a similar level of defense as the original PCI DSS requirement;
- Be "above and beyond" other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and
- Be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.

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.
Consumer - Individual purchasing goods, services, or both.
Critical systems / critical technologies - A system or technology that is deemed by the entity to be of particular importance. For example, a critical system may be essential for the performance of a business operation or for a security function to be maintained. Examples of critical systems often include security systems, public-facing devices and systems, databases, and systems that store, process, or transmit cardholder data. Considerations for determining which specific systems and technologies are critical will depend on an organization’s environment and risk-assessment strategy.
Data-Flow Diagram - A diagram showing how data flows through an application, system, or network.
Database - Structured format for organizing and maintaining easily retrievable information. Simple database examples are tables and spreadsheets.
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.
DSS - Acronym for “Data Security Standard.” See PCI DSS.
Dual Control - Process of using two or more separate entities (usually persons) operating in concert to protect sensitive functions or information. Both entities are equally responsible for the physical protection of materials involved in vulnerable transactions. No single person is permitted to access or use the materials (for example, the cryptographic key). For manual key generation, conveyance, loading, storage, and retrieval, dual control requires dividing knowledge of the key among the entities.
Encryption - Process of converting information into an unintelligible form except to holders of a specific cryptographic key. Use of encryption protects information between the encryption process and the decryption process (the inverse of encryption) against unauthorized disclosure.
Entity - Term used to represent the corporation, organization or business which is undergoing a PCI DSS review.
Firewall - Hardware and/or software technology that protects network resources from unauthorized access. A firewall permits or denies computer traffic between networks with different security levels based upon a set of rules and other criteria.
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.
HTTP - Acronym for “hypertext transfer protocol.” Open internet protocol to transfer or convey information on the World Wide Web.
HTTPS - Acronym for “hypertext transfer protocol over secure socket layer.” Secure HTTP that provides authentication and encrypted communication on the World Wide Web designed for security-sensitive communication such as web-based logins.
ID - Identifier for a particular user or application.
Index Token - A cryptographic token that replaces the PAN, based on a given index for an unpredictable value.
Information Security - Protection of information to insure 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 - Acronym for “internet protocol.” Network-layer protocol containing address information and some control information that enables packets to be routed and delivered from the source host to the destination host. IP is the primary network-layer protocol in the Internet protocol suite.
IP Address - Also referred to as “internet protocol address.” Numeric code that uniquely identifies a particular computer (host) on the Internet.
IP Address Spoofing - Attack technique used to gain unauthorized access to networks or computers. The malicious individual sends deceptive messages to a computer with an IP address indicating that the message is coming from a trusted host.
IPSEC - Abbreviation for “Internet Protocol Security.” Standard for securing IP communications at the network layer by encrypting and/or authenticating all IP packets in a communication session.
Issuer - Entity that issues payment cards or performs, facilitates, or supports issuing services including but not limited to issuing banks and issuing processors. Also referred to as “issuing bank” or “issuing financial institution.”
Issuing Services - Examples of issuing services may include but are not limited to authorization and card personalization.
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.
Least Privilege - Having the minimum access and/or privileges necessary to perform the roles and responsibilities of the job function.
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-approved activities, which results in the exploitation of system vulnerabilities. Examples include viruses, worms, Trojans (or Trojan horses), spyware, adware, and rootkits.
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. See Truncation for protection of PAN when stored in files, databases, etc.
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 five members of PCI SSC (American Express, Discover, JCB, MasterCard or Visa) as payment for goods and/or services. Note that a merchant that accepts payment cards as payment for goods and/or services can also be a service provider, if the services sold result in storing, processing, or transmitting cardholder data on behalf of other merchants or service providers. For example, an ISP is a merchant that accepts payment cards for monthly billing, but also is a service provider if it hosts merchants as customers.
MO/TO - Acronym for “Mail-Order/Telephone-Order.”
Monitoring - Use of systems or processes that constantly oversee computer or network resources for the purpose of alerting personnel in case of outages, alarms, or other predefined events.
Network - Two or more computers connected together via physical or wireless means.
Network Components - Include, but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.

Network Diagram - A diagram showing system components and connections within a networked environment.
Network Security Scan - Process by which an entity's systems are remotely checked for vulnerabilities through use of manual or automated tools. Security scans that include probing internal and external systems and reporting on services exposed to the network. Scans may identify vulnerabilities in operating systems, services, and devices that could be used by malicious individuals.
Network Segmentation - Also referred to as "segmentation" or "isolation." Network segmentation isolates system components that store, process, or transmit cardholder data from systems that do not. Adequate network segmentation may reduce the scope of the cardholder data environment and thus reduce the scope of the PCI DSS assessment.
Non-Consumer Users - Individuals, excluding cardholders, who access system components, including but not limited to employees, administrators, and third parties.
Off-the-Shelf - Description of products that are stock items not specifically customized or designed for a specific customer or user and are readily available for use.
Operating System / OS - Software of a computer system that is responsible for the management and coordination of all activities and the sharing of computer resources. Examples of operating systems include Microsoft Windows, Mac OS, Linux and Unix.
PA-DSS - Acronym for "Payment Application Data Security Standard."
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.
Patch - Update to existing software to add functionality or to correct a defect.
Payment Application - 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, 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. See also Acquirer.
PCI - Acronym for "Payment Card Industry."
PCI DSS - Acronym for "Payment Card Industry Data Security Standard."
PED - PIN entry device
Penetration Test - Penetration tests attempt to identify ways to exploit vulnerabilities to circumvent or defeat the security features of system components. Penetration testing includes network and application testing as well as controls and processes around the networks and applications, and occurs from both outside the environment (external testing) and from inside the environment.
Personally Identifiable Information - Information that can be utilized to identify an individual including but not limited to name, address, social security number, phone number, etc.
Personnel - Full-time and part-time employees, temporary employees, contractors, and consultants who are "resident" on the entity's site or otherwise have access to the cardholder data environment.
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-acceptance product, a POI consists of hardware and software and is hosted in acceptance equipment to enable a cardholder to perform a card transaction. The POI may be attended or unattended. POI transactions are typically integrated circuit (chip) and/or magnetic-stripe card-based payment transactions.
Policy - Organization-wide rules governing acceptable use of computing resources, security practices, and guiding development of operational procedures
Port - Logical (virtual) connection points associated with a particular communication protocol to facilitate communications across networks.
POS - Acronym for "point of sale." Hardware and/or software used to process payment card transactions at merchant locations.
Privileged User - Any user account with greater than basic access privileges. Typically, these accounts have elevated or increased privileges with more rights than a standard user account. However, the extent of privileges across different privileged accounts can vary greatly depending on the organization, job function or role, and the technology in use.
Procedure - Descriptive narrative for a policy. Procedure is the "how to" for a policy and describes how the policy is to be implemented.
PTS - Acronym for "PIN Transaction Security," PTS is a set of modular evaluation requirements managed by PCI Security Standards Council, for PIN acceptance POI terminals. Please refer to www.pcisecuritystandards.org.
Public Network - Network established and operated by a third-party telecommunications provider for specific purpose of providing data transmission services for the public. Data over public networks can be intercepted, modified, and/or diverted while in transit. Examples of public networks include, but are not limited to, the Internet, wireless, and mobile technologies. See also Private Network.
PVV - Acronym for "PIN verification value." Discretionary value encoded in magnetic stripe of payment card.
QSA - Acronym for "Qualified Security Assessor." QSAs are qualified by PCI SSC to perform PCI DSS on-site assessments. Refer to the QSA Qualification Requirements for details about requirements for QSA Companies and Employees.
Rainbow Table Attack - A method of data attack using a pre-computed table of hash strings (fixed-length message digest) to identify the original data source, usually for cracking password or cardholder data hashes.
Remote Access - Access to computer networks from a remote location. Remote access connections can originate either from inside the company's own network or from a remote location outside the company's network. An example of technology for remote access is VPN.
Reseller / Integrator - An entity that sells and/or integrates payment applications but does not develop them.
Risk Analysis / Risk Assessment - Process that identifies valuable system resources and threats; quantifies loss exposures (that is, loss potential) based on estimated frequencies and costs of occurrence; and (optionally) recommends how to allocate resources to countermeasures so as to minimize total exposure.
ROC - Acronym for "Report on Compliance." Report documenting detailed results from an entity's PCI DSS assessment.
Rootkit - Type of malicious software that when installed without authorization, is able to conceal its presence and gain administrative control of a computer system.

Router - Hardware or software that connects two or more networks. Functions as sorter and interpreter by looking at addresses and passing bits of information to proper destinations. Software routers are sometimes referred to as gateways.
Sampling - The process of selecting a cross-section of a group that is representative of the entire group. Sampling may be used by assessors to reduce overall testing efforts, when it is validated that an entity has standard, centralized PCI DSS security and operational processes and controls in place. Sampling is not a PCI DSS requirement.
SAQ - Acronym for "Self-Assessment Questionnaire." Reporting tool used to document self-assessment results from an entity's PCI DSS assessment.
Schema - Formal description of how a database is constructed including the organization of data elements.
Scoping - Process of identifying all system components, people, and processes to be included in a PCI DSS assessment. The first step of a PCI DSS assessment is to accurately determine the scope of the review.
SDLC - Acronym for "system development life cycle." Phases of the development of a software or computer system that includes planning, analysis, design, testing, and implementation.
Security Policy - Set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.
Sensitive Area - Any data center, server room or any area that houses systems that stores, processes, or transmits cardholder data. This excludes the areas where only point-of-sale terminals are present such as the cashier areas in a retail store.
Sensitive Authentication Data - Security-related information (including but not limited to card validation codes/values, full track data (from the magnetic stripe or equivalent on a chip), PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.
Separation of Duties - Practice of dividing steps in a function among different individuals, so as to keep a single individual from being able to subvert the process.
Server - Computer that provides a service to other computers, such as processing communications, file storage, or accessing a printing facility. Servers include, but are not limited to web, database, application, authentication, DNS, mail, proxy, and NTP.
Service Code - Three-digit or four-digit value in the magnetic-stripe that follows the expiration date of the payment card on the track data. It is used for various things such as defining service attributes, differentiating between international and national interchange, or identifying usage restrictions.
Service Provider - Business entity that is not a payment brand, directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This also includes companies that provide services that control or could impact the security of cardholder data. Examples include managed service providers that provide managed firewalls, IDS and other services as well as hosting providers and other entities. If an entity provides a service that involves only the provision of public network access—such as a telecommunications company providing just the communication link—the entity would not be considered a service provider for that service (although they may be considered a service provider for other services).
Smart Card - Also referred to as "chip card" or "IC card (integrated circuit card)." A type of payment card that has integrated circuits embedded within. The circuits, also referred to as the "chip," contain payment card data including but not limited to data equivalent to the magnetic-stripe data.
Spyware - Type of malicious software that when installed, intercepts or takes partial control of the user's computer without the user's consent.
System Components - Any network component, server, or application included in or connected to the cardholder data environment.
Threat - Condition or activity that has the potential to cause information or information processing resources to be intentionally or accidentally lost, modified, exposed, made inaccessible, or otherwise affected to the detriment of the organization.
Token - In the context of authentication and access control, a token is a value provided by hardware or software that works with an authentication server or VPN to perform dynamic or two-factor authentication.
Track Data - Also referred to as "full track data" or "magnetic-stripe data." Data encoded in the magnetic stripe or chip used for authentication and/or authorization during payment transactions. Can be the magnetic-stripe image on a chip or the data on the track 1 and/or track 2 portions of the magnetic stripe.
Transaction Data - Data related to electronic payment card transaction.
Trojan - Also referred to as "Trojan horse." A type of malicious software that when installed, allows a user to perform a normal function while the Trojan performs malicious functions to the computer system without the user's knowledge.
Truncation - Method of rendering the full PAN unreadable by permanently removing a segment of PAN data. Truncation relates to protection of PAN when stored in files, databases, etc. See Masking for protection of PAN when displayed on screens, paper receipts, etc.
Virtual Payment Terminal - A virtual payment terminal is web-browser-based access to an acquirer, processor or third-party service provider website to authorize payment card transactions, where the merchant manually enters payment card data via a securely connected web browser. Unlike physical terminals, virtual payment terminals do not read data directly from a payment card. Because payment card transactions are entered manually, virtual payment terminals are typically used instead of physical terminals in merchant environments with low transaction volumes.
VPN - Acronym for "virtual private network." A computer network in which some of connections are virtual circuits within some larger network, such as the Internet, instead of direct connections by physical wires. The end points of the virtual network are said to be tunneled through the larger network when this is the case. While a common application consists of secure communications through the public Internet, a VPN may or may not have strong security features such as authentication or content encryption. A VPN may be used with a token, smart card, etc., to provide two-factor authentication.
Web Application - An application that is generally accessed via a web browser or through web services. Web applications may be available via the Internet or a private, internal network.