UNLV Payment Card Merchant Policy
Credit 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 credit 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, or transmit cardholder data and/or sensitive authentication 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 processes, transmits, or stores cardholder data (CHD). All merchants at the University are required to use the NSHE contracted merchant services provider (currently Wells Fargo Bank) 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 Banking and Investments Office and the University's merchant services provider. The Controller's Office relies on the NSHE contracted merchant services provider to ensure that web payment gateway vendors are PCI compliant.

Although the primary focus of the PCI DSS is on Internet-based sales, there are other services that allow systems to be Internet accessible which may expose cardholder information. Basic functions such as e-mail can result in Internet accessibility of a merchant's network. Therefore, all university merchants, including merchants transmitting via a terminal on a dedicated phone line, must complete an annual Self- Assessment Questionnaire (SAQ) and, if applicable, an internal scan and a remote external scan by our PCI approved vendor.

Purpose

This Policy defines the steps that Payment Card Merchant account holders and eCommerce users at UNLV must use to access and secure payment card data in all forms. 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 the storage, transmission, and processing of payment card data.

Periodic reviews of merchants 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 card holder's data, self-assessment procedures, and processing procedures may lose the privilege to serve as a merchant.

Compliance requirements for each merchant are determined based on the type and volume of payment card transactions. All business units which accept payment cards will be required to complete an annual self-assessment questionnaire which will be coordinated by the Controller's Office which will coordinate completion and filing of any required reports with the University's merchant services provider.

Policy Statement

Who Should Know This Policy

Any official or administrator with responsibilities for managing University payment card transactions and those employees entrusted with handling cardholder data must be aware of this policy. This includes fiscal officers 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 connected to a telephone line 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. This policy also applies to the use of wireless devices for payment acceptance.

Business units wishing to accept credit card payments must comply with the Payment Card Industry Data Security Standards (PCI-DSS). These 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
- 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 Credit Card Merchants

All merchants must comply with the requirements listed in the section below titled "General Responsibilities for all Departments utilizing Credit Card Merchant Accounts." These responsibilities include PCI DSS requirements and University requirements. In addition, merchants must refer to the specific requirements listed in the "Credit 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.
- **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 Credit Card Handlers and Processors" (Appendix A) and make the necessary additions pertaining to your department's credit 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. (PCI DSS 9)
- **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 Credit Card Handlers and Processors" form** for all personnel involved in credit card transactions. (PCI DSS 12.6)
- **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. (PCI DSS. 7.1)
- **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. (PCI DSS 8.1)
- **Transmitting cardholder data by e-mail, chat or FAX prohibited** – Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc) (PCI DSS 4.2)
- **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). (PCI DSS 3.2)
- **Segregation of duties** - Establish appropriate segregation of duties between personnel processing transactions, issuing refunds, 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 Primary Account Number (PAN). (PCI DSS 3.3)

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.
- Use of wireless data network for payment card processing is not allowed (cellular card terminals are permissible, however).
- Cardholder data must never be transmitted via email and departments should not solicit cardholder data to be returned via e-mail..
- Cardholder data inadvertently received by e-mail should be deleted immediately and 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 form of transmittal to protect your card information. "
- All documentation containing cardholder data must be destroyed in a manner that will render them unreadable 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 monthly report of activity (by day and in total) is to be generated and 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 assure 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.
- 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

- Departmental procedures should be reviewed, signed and dated by the Department Head or Business Manager on an annual basis and submitted to the Controller's Office along with other required PCI compliance documentation.
- For assistance in developing departmental procedures, contact the Controller's Office at 895-1142.

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 sales drafts provided in the new merchant kit. Get an imprint of the card; write a description of the transaction, the transaction date, and the dollar amount on the draft. Also write the merchant name on the sales draft. Be sure to have the cardholder sign and give him/her a copy of the draft. Hand enter the information when the terminal is up and running again. Keep the original copy of the sales draft in case a retrieval request is received.
- Inspect the terminal or card swipe mechanism daily to insure it has not been tampered with.
- Terminal or card swipe mechanism is stored securely overnight.

Mail-in, Fax and Phone Orders

- Maintain a payment listing for balancing and accounting purposes but this listing should not contain the cardholder data –the last four digits of the card number may be listed.
- Fax machines 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.
- 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 (such as Authorize.net or Touchnet) and the account must be opened by the Controller's Office in accordance with NSHE Banking and Investment Office policy.
- No cardholder data can be stored on UNLV servers or networks.
- Review and comply with UNLV's "UserID and Password Policy for Credit Card Processing" available on the Controller's website.
- 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 Linda Kim at 895-1142.
- Periodic network vulnerability scans will be conducted and the department is responsible for timely remedy of deficiencies.
- 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.

Sales Draft Requests / Chargebacks

Sales Draft Requests

- Sales Draft Requests will be sent to the Controller's Office from the University's merchant services provider when a customer wants more information or is disputing a transaction.
- The Controller's Office will forward these requests to the Department for response. There is a limited amount of time for the Department to respond so promptness is critical.
- The Department will send the required documentation to Wells Fargo in response to the request and maintain a copy of submitted material along with the Sales Draft Request form. The date materials were submitted should be documented.

Chargebacks

- A chargeback is when a customer has disputed a payment card transaction and the Department has either not been able to supply documentation to substantiate that transaction or has not done so on a timely basis. A chargeback is a reduction of your revenue.
- Departments should periodically review their chargebacks to see if there are internal policies that need to be changed so that fewer transactions are disputed.
- Chargeback forms should be maintained in the department and a note made in the customer's file of the chargeback and the circumstances.

APPENDIX A

Responsibilities of Credit Card Handlers and Processors

(Supervisors – please copy this section and have all staff members involved in the handling of cardholder data return a signed copy to you. Keep these copies on file.)

As a 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 credit primary account number, three (3) or four (4) digit validation code (usually on the back of payment cards), or PINs (personal identification numbers).
2. Transmit cardholder's data by e-mail or fax.
3. Electronically store cardholder data on a University computer file or server.
4. Share a computer login or password if I have access to a computer used to process cardholder data.

I will DO the following:

1. At time of employment, agree to complete a background check within the limits of local law.
2. Change a vendor-supplied or default password if I have access to a computer with cardholder data.
3. 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.
4. Escort and supervise all visitors including UNLV personnel in areas where cardholder data is maintained.
5. Store all physical documents or storage media containing card holder data in a locked drawer, locked file cabinet, or locked office.
6. Immediately report a payment card security incident to my supervisor and the Controller's Office if I know or suspect credit card information has been exposed, stolen, or misused.
   a. Notification to the Supervisor should be in writing
   b. Notification to the Controller's Office should be by e-mail to linda.kim@unlv.edu.

   (This report must not disclose by fax or e-mail any cardholder data, three or four digit validation codes, or PIN numbers. It must include a department name and contact number.)

______________________________ ______________________________
Signature Date

____
Print Name

APPENDIX B

PCI DEFINITIONS AND LINKS

AOC – Attestation of Compliance – Used by level 2-4 merchants to validate compliance to their acquirer or bank.

Anti-Virus Program – Programs capable of detecting, removing, and protecting against various forms of malicious code or malware, including viruses, worms, Trojan horses, spyware, and adware.

Application – Includes all purchased and custom software programs or groups of programs designed for end users, including both internal and external (web) applications.

ASV – Approved Scanning Vendor. Company approved by the PCI Council to perform the required quarterly vulnerability scans.

Authentication – Process of verifying identity of a subject or process.

Authorization – Granting of access or other rights to a user, program, or process.

Cardholder – Customer to whom a card is issued or individual authorized to use the card

Cardholder Data – Full magnetic stripe or the PAN plus any of the following:

- Cardholder name
- Expiration date
- Service Code

Cardholder Data Environment – Area of computer system network that possesses cardholder data or sensitive authentication data and those systems and segments that directly attach or support cardholder processing, storage, or transmission. Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data from those that do not, may reduce the scope of the cardholder data environment and thus the scope of the PCI assessment.

Card Validation Value or Code – Code element on a card's magnetic stripe that uses secure cryptographic process 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)
- **CVC** Card Validation Code (MasterCard payment cards)
- **CVV** Card Verification Value (Visa and Discover payment cards)
- **CSC** Card Security Code (American Express)

CISP – Card Information Security Program. Visa's payment card security program.

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 1) meet the intent and rigor of the original stated PCI DSS requirement; 2) repel a compromise attempt with similar force; 3) be "above and beyond" other PCI DSS requirements (not simply in compliance with other PCI DSS requirements); and 4) be commensurate with the additional risk imposed by not adhering to the PCI DSS requirement.

Compromise – Intrusion into computer system where unauthorized disclosure, modification, or destruction of cardholder data is suspected.

Credit Card Authorization Form – A form that is downloaded from a website, part of a brochure or any other document that solicits cardholder data to be returned in person, by regular mail or secure FAX.

DISC – Discover Information Security Program. Discover Card's payment security program.

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, software, or unauthorized disclosure.

Firewall – Hardware both that protect resources of one network from intruders from other networks. Typically, an enterprise with an intranet that permits workers access to the wider Internet must have a firewall to prevent outsiders from accessing internal private data resources.

IP Internet Protocol – Network layer protocol containing address information and some control information that enables packets to be routed. IP is the primary network-layer protocol in the Internet protocol suite.
IP Address – Numeric code that uniquely identifies a particular computer on the Internet
Magnetic Stripe Data (Track Data) – Data encoded in the magnetic stripe used for authorization during transactions when the card is presented. Entities must not retain full magnetic stripe data subsequent to transaction authorization. Specifically, subsequent to authorization, service codes, discretionary data/ Card Validation Value/Code, and proprietary reserved values must be purged; however, account number, expiration date, name, and service code may be extracted and retained, if needed for business.
Malware Malicious software. Designed to infiltrate or damage a computer system, without the owner's knowledge or consent.
Monitoring Use of system that constantly oversees a computer network including for slow or failing systems and that notifies the user in case of outages or other alarms.
Data (Track Data) Data encoded in the magnetic stripe used for authorization during transactions when the card is presented. Entities must not retain full magnetic stripe data subsequent to transaction authorization. Specifically, subsequent to authorization, service codes, discretionary data/ Card Validation Value/Code, and proprietary reserved values must be purged; however, account number, expiration date, name, and service code may be extracted and retained, if needed for business**.**
Merchant – the entity that is authorized by a bank acquirer to accept credit cards for payment.
Merchant Level – Defined by the number of transactions (not dollar amount) a merchant completes in 1 year. Denotes the way a merchant must validate compliance.
Network – Two or more computers connected together to share resources
Network Components – Includes, but are not limited to firewalls, switches, routers, wireless access points, network appliances, and other security appliances.
Payment Cardholder Environment – That part of the network that possesses cardholder data or sensitive authentication data.
PAN – Primary Account Number is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account. Also called Account Number.
Password – A string of characters that serve as an authenticator of the user.
Scan – Automated tool that remotely checks merchant or service provider systems for vulnerabilities. Non-intrusive test involves probing external-facing systems based on external-facing IP addresses and reporting on services available to external network (that is, services available to the Internet). Scans identify vulnerabilities in operating systems, services, and devices that could be used by hackers to target the company’s private network
PABP – Payment Applications Best Practices. The Visa program replaced by PA-DSS.
PA-DSS – Payment Application Data Security Program. Replaces the PABP.
Patch – Quick repair job for piece of programming. During software product beta test or try-out period and after product formal release, problems are found. A patch is provided quickly to users.
PCI DSS – Payment Card Industry Data Security Standard
PCI PED – Payment Card Industry Pen Entry Device
PCI SSC – Payment Card Industry Security Standards Council – the governing body of the standard.
Penetration – Successful act of bypassing security mechanisms and gaining access to computer system.
Penetration Test – Security-oriented probing of computer system or network to seek out vulnerabilities that an attacker could exploit. Beyond probing for vulnerabilities, this testing may involve actual penetration attempts. The objective of a penetration test is to detect identify vulnerabilities and suggest security improvements.
PIN – Personal Identification Number
Policy – Organization-wide rules governing acceptable use of computing resources, security practices, and guiding development of operational procedures.
POS – Point of Sale
Procedure – Descriptive narrative for a policy. Procedure is the “how to” for a policy and describes how the policy is to be implemented.

Public Network – The network established and operated by a telecommunications provider or recognized private company, for specific purpose of providing data transmission services for the public. Data must be encrypted during transmission over public networks as hackers easily and commonly intercept, modify, and/or divert data while in transit. Examples of public networks in scope of PCI DSS include the Internet, GPRS, and GSM.

QSA – Qualified Security Assessor - Person certified by the PCI SSC to assist merchants with compliance.

Risk Analysis – Process that systematically 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.

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.

ROC – Report on Compliance. Tool used by level 1 merchant to prove compliance. Must be completed by a QSA.

SAQ – Self Assessment Questionnaire. The tool a merchant uses to analyze and report their compliance

SDP – MasterCard’s security program.

Security Policy -- Set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Sensitive Authentication Data – Security-related information (Card Validation Codes/Values, complete track data, PINs, and PIN Blocks) used to authenticate cardholders, appearing in plaintext or otherwise unprotected form. Disclosure, modification, or destruction of this information could compromise the security of a cryptographic device, information system, or cardholder information or could be used in a fraudulent transaction.

Server – Computer that provider 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, authentication, DNS, mail, proxy, and NTP.

Service Code – Three or four-digit number on the magnetic-stripe that specifies acceptance requirements and limitations for a magnetic-stripe read transaction.

Service Provider – Business entity that is not a payment card brand member or a merchant directly involved in the processing, storage, transmission, and switching or transaction data and cardholder information or both. This also includes companies that provide services to merchants, services providers or members 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. Entities such as telecommunications companies that only provide communication links without access to the application layer of the communication link are excluded.

SQL – Structured Query Language. Computer language used to create, modify, and retrieve data from relational database management systems.

SQL Injection – Form of attack on database-driven web site. An attacker executes unauthorized SQL commands by taking advantage of insecure code on system connected to the Internet. SQL injection attacks are used to steal information from a database from which the data would normally not be available and/or to gain access to an organization’s host computers through the computer that is hosting the database.

Truncation – Practice of removing data segment. Commonly, when account numbers are truncated, the first 12 digits are deleted, leaving only the last 4 digits.

Virus – Program or string of code that can replicate itself and cause modification or destruction of software or data.

Vulnerability – Weakness in system security procedures, system design, implementation, or internal controls that could be exploited to violate system security policy.

Vulnerability Scan – Scans used to identify vulnerabilities in operating systems, services, and devices that could be used by hackers to target the company’s private network.

XSS – Cross-site Scripting. Type of security vulnerability typically found in web applications. Can be used by an attacker to gain elevated privilege to sensitive page content, session cookies, and variety of other objects.