UNL PAYMENT CARD POLICIES AND PROCEDURES

Table of Contents

Updated: November, 2011

UNL PAYMENT CARD POLICY AND PROCEDURES

Payment Card Merchant Security Standards Policy and Procedures

Policy: We will assure the protection of cardholder data and effect the proper execution of cardholder transactions.

Procedures:

1. University of Nebraska –Lincoln payment card merchants' procedures comply with the current Payment Card Industry Data Security Standards (PCIDSS) (see under separate cover)

    a. Bursar approves merchants
        - Bursar logs in, processes, and logs out merchant applications
    b. New "Merchants" must successfully complete the assessment questionnaire to assure their understanding of the requirements to comply with payment card merchant safeguards
    c. Merchants must annually complete the assessment questionnaire and other required compliance documents to assure understanding of the requirements to comply with payment card merchant safeguards
        - Bursar logs in, processes, and logs out merchant compliance documentation

2. Bursar will certify that electronic scans of merchant networks are done quarterly

    a. On-site compliance testing done randomly at least annually

3. UNL PCIDSS Policies and Procedures will be reviewed annually for updates/modifications

4. Annual review of merchants, by Bursar, to assure each has sufficient activity and resources to warrant payment card merchant status

5. Any Breach of Security must be reported immediately to Information Services at http://is.unl.edu under Help section "Report Computer Security Incident."

6. Bursar sends quarterly reminders to merchants regarding standard security precautions and current merchant information. These will address such things as restricting access, safeguarding passwords and other minimum standards.

Introduction

The main function of the information in this manual is to assist campus entities who are interested in becoming payment card merchants (internet or Point of Sale) by accepting payment cards as a form of payment, want to enhance their internet merchant sites or improve their Point of Sale (POS) processes. The information describes not only how to get started, but outlines UNL policies and procedures that need to be followed to continue to offer credit cards as a payment choice.

Credit Card payments can be accepted using any of the following:

- Secure website – Internet – E-Commerce **(e-mail is not acceptable)**
- Over the counter (in person)
- Telephone/Facsimile
- Mail

If a department wishes to accept payment cards, it must comply with the Payment Card Industry Data Security Standards (PCIDSS). The standards are based on best data security practices, and as such, will go a long way to protect all other critical information. Payment Card Industry (or PCI) compliance mitigates risk, protects against the costs of a breach, and strengthens overall security. When a university complies with the PCIDSS, it not only protects itself, but also its students, employees, alumni and customers.

Compliance by all merchants must be achieved and documented ANNUALLY. The Bursar's Office will contact merchants each year in March to inform them of the requirements and deadlines which must be met. Non-compliance will result in the loss of merchant services.

This policy and these procedures should be known by any official or administrator with responsibilities for managing University payment card transactions and those employees who are entrusted with handling payment cards and payment card information.

Payment Card Industry Data Security Standard

- See Separate Policies at: https://www.pcisecuritystandards.org/

Definitions

Acquirer — A financial institution which is a bankcard association member that initiates and maintains relationships with merchants that accept payment cards. UNL's Acquirer is TSYS Merchant Solutions (TSYS) which was formerly First National Merchant Solutions.

Cardholder Data — Includes four components:

- Primary Account Number (PAN)
- Service Code -3 or 4 digit number in the magnetic stripe
- Cardholder name
- Expiration Date

Cardholder Data Environment — The people, processes and technology that store, process or transmit cardholder data or sensitive authentication data, including any connected system components

Cardholder Verification Value (CVV2) — Also known as Card Validation Code or Value, or Card Security Code. Refers to either: (1) magnetic-stripe data, or (2) printed security features like the 3 or 4 digit code number printed on the back of the card

Chargeback — Also known as a "Debit Memo," a reversal of a sales transaction. If you deposited a $50 transaction in your merchant bank account, a chargeback for that transaction indicates that the $50 has been debited from your merchant account.

E-Commerce — Transactions entered at a website.

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.

Payment Cards — "Branded" cards used to pay for goods or services with the card type logo on the face of the card – such as Visa or MasterCard. We do not accept ATM or pin-based debit cards.

PCI — Payment Card Industry - Used when referring to the Payment Card Industry Data Security Standard.

Point-of-Sale (POS)	Generally a card present transaction or manually entered card number. Not entered at a website.
SAQ	Acronym for "Self-Assessment Questionnaire." Tool used by any entity to validate its compliance with the PCI DSS.
Terminal	POS device used to gather the magnetic strip data from the card and print the receipt to be signed by the customer.
Truncation	The practice of removing a data segment. Commonly, when account numbers are truncated, the first 12 digits are deleted, leaving only the last 4 digits.
Virtual Terminal	A virtual 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 terminals do not read data directly from a payment card. Because payment card transactions are entered manually, virtual terminals are typically used instead of physical terminals in merchant environments with low transaction volumes.
Vulnerability	Flaw or weakness which, if penetrated, breached or exploited, may result in an intentional or unintentional compromise of a system.

Resources

Bursar's Office: bursar@unlnotes.unl.edu

Hellwege, Jennifer –Assistant Bursar
jhellwege2@unl.edu (402) 472-9004

- Documentation
- Equipment & Service Provider Acquisition
- Income/Expense Distribution
- Internal Controls
- Merchant Retrieval Requests
- Network Scan Results
- Procedure Development
- Record Management
- Third Party Providers
- Transaction Processing

Information Services (IS):

Eitzmann, Kent –Network Coordinator
keitzmann1@unl.edu (402) 472-5665

- Networking

Rutt, Mike –Senior Information Security Analyst
mrutt2@unl.edu (402) 472-0933

- Network Scan Remediation
- Server Security
- Technological Support

Other Resources:

TSYS Merchant Solutions	www.tsys.com
Visa	usa.visa.com
MasterCard	www.mastercard.com/us
Discover	www.discovernetwork.com
PCI Security Standards Council	www.pcisecuritystandards.org/

Becoming a Merchant

Information regarding start-up and on-going costs is provided below. Carefully consider the costs involved with accepting credit card payments and evaluate whether or not it is a benefit to your department to offer this as a payment option. Any University Department that wishes to accept payment cards must complete an "Application to Become a Merchant" and submit it to the Bursar for approval by the Assistant Vice Chancellor – Financial Services. Minimum processing requirements, which incorporate mandatory internal controls, also must be outlined. One part of the application is to describe the processes the Department will employ to safeguard cardholder data. The information in this manual should be thoroughly reviewed prior to submitting an application.

Once the request has been approved, the Bursar's Office will notify and work with the department and TSYS Merchant Solutions (TSYS) to begin the set up procedures to obtain a merchant number. Information Services will contact the technical support staff for e-commerce merchants. It will take approximately three to four weeks, from obtaining merchant approval, to actually be up and processing payment card transactions. TSYS offers free training via the phone for POS merchants which covers:

- How to run a transaction, swiped and key entered.
- How to credit and void transactions. (Keep in mind, this activity must be done by someone other than the person responsible for the sale.)
- Getting an imprint of any key entered transactions
- How to manually batch the terminal at the end of the day. (The terminals are however set to auto batch close at midnight if you forget to do it manually.)
- All of the prompts the terminal will bring up when phone orders are taken (i.e. the AVS –address verification)

Estimated Start-up and On-going Costs for Payment Card Merchants
(Subject to change without notice)

Point-of-Sale Costs:

Initial Costs	
Equipment -VeriFone Vx570	$300 each
Activate Port	$ 0
Pull wire for new Phone/modem*	$200/1; $250/2
On-Going Costs	
Monthly Phone Line Cost*	$30
Monthly Port Charge	$ 4.25-7.00

Bank/Processor charges are 2-3% of sales.

*A dedicated telephone line is needed for a modem for POS payment card equipment. It will access only 800 numbers so it must have access to long distance.

E-Commerce Costs:

Initial Costs	
Payment Processor setup** (ex. Verisign, Cybersource)	$100

On-Going Costs	
Monthly maintenance	$5 – $50
Per transaction charges	$.05 - $.15

Bank/Processor charges are 2-3% of sales.

**Costs will vary depending on application and/or processor selected. Contact the Bursar's Office for assistance/approval of selections.

Minimum Data Processing Internal Controls

- Separate, to the extent possible, all duties related to data processing of payment card information. A system of checks and balances should exist where tasks are performed by different individuals in order to assure adequate controls.

  For example, the same person should not process credit card transactions and perform the monthly merchant statement reconciliation. The same person should not process transactions and refunds. The following duties should be performed by different individuals:

  1) payment card refund,
  2) transaction processing
  3) departmental oversight and review

- University personnel who receive and/or process credit card information must properly safeguard the data and record the transaction(s). This applies to all personnel who handle cardholder information during the processing of any transaction, or who retain, store, safeguard and/or dispose of the information.

  Payment card documentation should be treated much like cash. It should be maintained in a secure environment limited to the minimum number of dependable, trustworthy and accountable staff. Secure environments include locked drawers, locked file cabinets, file cabinets in locked offices and safes.

- Information Services (IS) must review and approve implementation of technology used to process any payment card transaction. This includes all aspects of the interface between the customer and the University's systems.
- Criminal background checks must be performed on any new or transferring employees who will be permitted to handle cardholder data. There should be no outstanding or unexplained items resulting from this check.
- All credit card terminals and web applications must be closed out and reconciled on a daily basis. Departments are also responsible for responding to any disputes, chargebacks and retrieval requests within the timeframes specified on the requests.
- Merchants will keep an original or imaged copy of each payment card transaction for no less than 18 months. After 18 months, these must be destroyed in a manner that will render them unreadable.
- The Department will be responsible for any losses, penalties or punitive expenses due to inadequate internal controls.

Application for Merchant Account

- See separate document under **"Forms"** available at bf.unl.edu/bursarpolicy/CreditCardProcessing.shtml

General Procedures for On-going Operations

Any exception to the procedures outlined below MUST be discussed and approved by the Bursar and Information Services **prior** to implementation.

All Payment Card Transaction Types

- Do not disclose or acquire any cardholder information without the cardholder's consent.
- Keep all cardholder numbers and information secure and confidential and limit access to a minimum number of employees.
- Cardholder data cannot be stored in any fashion on UNL computers, networks or related media.
- Use of wireless internet for payment card processing is not allowed.
- Payment card numbers must not be transmitted via email.
- All documentation containing card account numbers must be destroyed in a manner that will render them unreadable after their useful life (18 months) has expired.
- A once a month report of activity (by day and in total) is to be generated and submitted to the Bursar's Office by the 10th of each month. This report should include your merchant name and number, the daily totals by batch, sales distribution, and total for the month. A sample report is available from the Bursar's Office.
- The Bursar's Office will balance the Departmental reports with the monthly merchant statements from TSYS and post a monthly journal entry to allocate sales and fees to each Merchant. Each Merchant will receive documentation from the Bursar's Office on the journal entries done. This is done during the month following the sales activity.
- Reconcile daily activity to merchant statements at least monthly to assure credit is received for all processed transactions. Verify amount to Bursar postings. Retain documentation in the Department that a reconciliation was done.
- Initial and subsequent training sessions will be coordinated by the Bursar's Office. All employees who process or oversee payment card transactions will be required to attend. Failure to attend can result in loss of merchant processing privileges.
- Each department must have written payment card processing procedures specific to its organization. For assistance in developing departmental procedures, contact the Bursar's Office at 472-9004 or bursar@unlnotes.unl.edu The procedures must include, but are not limited to, the following:

    a. Segregation of duties
    b. Reconciliation procedures – daily and monthly
    c. Physical security
    d. Disposal

- Departmental procedures should be reviewed, signed and dated by the Department Head or Business Manager on an annual basis and submitted to the Bursar's Office along with other required PCI compliance documentation.
- Annual update of Merchant Information including current contacts is required.

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 a duplicate copy to the cardholder (unless operating with no-signature feature for transactions under $25).
- 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 to be provided to the Bursar's Office by the 10th of each month.
- 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.

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 until needed for balancing the day's transactions. If possible, the PAN should be destroyed from paperwork after processing is complete. Thought should be given to the design of your payment form to accomplish this. If the PAN is positioned in a way that it can be removed from the remainder of the form, the payment portion could then be handled in a manner consistent with PCI while the remainder of the form can be independently processed. This minimizes our risk.
- 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 to be provided to the Bursar's Office by the 10th of each month.

Internet (E-Commerce) Orders

- All payment card transactions must be processed by a PCIDSS compliant third-party provider such as PayPal/Verisign. Documentation of their compliance must be on file with UNL.
- No payment card data can be stored on UNL servers or networks.
- Review and comply with UNL's "UserID and Password Policy" available at bf.unl.edu/bursarpolicy/CreditCardProcessing.shtml
- Documented approval from IS that systems and technology used meet all required security protocols should be kept on file in the department. This approval will be obtained by contacting Mike Rutt of IS at mrutt2@unl.edu
- Periodic network vulnerability scans will be conducted and the department is responsible for timely remedy of deficiencies.
- Complete "System Configuration Change Request" (available at bf.unl.edu/bursarpolicy/CreditCardProcessing.shtml) prior to implementing any technology changes and submit form to Bursar, IS Security and IS Networking. The form must be approved by IS prior to any change being made.

Sales Draft Requests / Chargebacks

Sales Draft Requests

- Sales Draft Requests will be sent to the Bursar's Office from TSYS when a customer wants more information or is disputing a transaction.
- The Bursar'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 TSYS the required documentation as instructed on the form 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 credit card transaction and the Department has either not been able to supply documentation to substantiate the transaction or has not done so on a timely basis. A chargeback is a reduction of your revenue.
- Chargeback Advices will be sent to the Bursar's Office from TSYS. The Bursar's Office will forward these to the Department. The Department

may choose to contest the chargeback. There is a limited amount of time for the Department to respond so promptness is critical.

- Departments should periodically review their chargebacks to see if there are internal policies that need to be changed so fewer transactions are disputed. Common things to consider are: 1) the return policy should be clear to the customer and 2) the department name appearing on the customer's statement should be disclosed to the customer.
- Chargeback forms should be retained in the department and a note made in the customer's file of the chargeback and the circumstances surrounding it.

Compliance Documentation Requirements

Beginning in January 2007, the University was classified a Level 3 merchant by our acquiring bank, First National Bank Omaha or FNNI. We must document our PCIDSS compliance with them annually. All of our merchants, approximately 40, must be compliant for the University to continue to offer payment cards as a payment option.

All compliance documentation will be distributed, maintained and cataloged by the Bursar's Office. **Failure to submit documents in a timely manner will result in loss of merchant privileges.** The documentation required for compliance is:

Self Assessment Questionnaire (SAQ)

An SAQ must be completed and returned to the Bursar annually. The Bursar's Office will provide you the appropriate SAQ version for each year's assessment. Each merchant will determine the SAQ type which applies to their business activities. Upon review of all compliance documentation, the Bursar/IS may require a different SAQ type. The SAQ must be signed by the department head.

Procedural Documentation

Departmental procedures must be submitted to the Bursar's Office annually. Guidelines for this documentation are discussed under "General Procedures for On-going Operations". They must be signed by the department head indicating compliance with UNL Payment Card Policies and Procedures. Review and evaluate them annually.

Merchant Data Updates

There is a separate Merchant Profile Form for paper merchants and internet merchants. Complete the form applicable for your merchant number(s). The form is available at: bf.unl.edu/bursarpolicy/CreditCardProcessing.shtml These are to be updated and submitted to the Bursar's Office annually. They should be signed by the department head indicating they are current.

Quarterly Network Scans

The Bursar schedules quarterly scans and any necessary followup scan necessary to obtain a passing scan for submission to TSYS. Results will be referred to the department for remediation. Merchants will be required to respond with remediation plans within three business days and then develop timely implementation schedules. A PASSing PCI scan must be submitted each quarter to

maintain compliance with TSYS. For a scan to be PASSing, no merchants can have any FAILs. So it is imperative issues are resolved promptly.

Incident Response Plan

Reporting a Breach of Security

Any incidence must be immediately reported at http://is.unl.edu. Go to the "Faculty & Staff" page. Select "Report Information Security Incidents" under the "Security" section.

If you suspect a security incident has occurred that could impact the University's network, computers or data, you are required to report the incident immediately.

Using this on-line form is the fastest and most efficient way to get your situation addressed and to notify the right people for response.

If you suspect loss or theft of any materials containing cardholder data, you must immediately notify all three of the following parties:

1. UNL Police (Emergency number 402-472-3550 and Non-emergency number 402-472-3555)
2. The Bursar's Office (402-472-1734 daily or 402-440-2444 after 5:00 pm)
3. Your supervisor

Items Under Separate Cover

E-Commerce Security Policy

UserID and Password Policy

System Configuration Change Request

Merchant Profile Form