Payment Cards Processing at UNL

VOLUME 19, ISSUE 2 APRIL, 2024

University of Nebraska-Lincoln

PCI Compliance Paperwork Due Friday, May 17th

The first step in PCI compliance is to collect each merchant account's compliance paperwork. The same documentation as in past years will be required: **Merchant Profile** and **Procedures Document with Cardholder Data (CHD) Flowchart**. Merchants will also need to do a SAQ, coming soon (see page 2). PCI DSS v4.0 went into effect on March 31st. The new PCI standards will require eCommerce SAQ-A merchants to provide a site scan as part of the SAQ (see page 2).

How do you get started? For each merchant account, you need to review, update, and submit:

- **Merchant Profile** – FY 2023-24 forms are available here: http://pci.unl.edu/merchant-profile (please use the current forms as fields may have changed)
- **Procedures Document with a current CHD Flowchart** – narrative (no standard form)

REMINDER: Do not combine merchant accounts on these documents. We need a completed profile and procedures document for each merchant account/number.

Create a PCI FY 23-24 folder for retaining your documents. Download the current Merchant Profile form here: http://pci.unl.edu/merchant-profile

Access last year's PCI FY 22-23 files. Review last year's documents and update information to accurately reflect this year's processes. Save the updated documents in your new folder. New merchants will need to create all documentation. The procedures document is a narrative of your processes and should incorporate the following:

- make, model, serial number and location of all equipment*
- details of all payment channels
- storage/purge details of cardholder data (if appl.)
- demonstration of segregation of duties in place
- flowchart of cardholder data
- individuals involved in payment processing
- staff training requirements
- information on reconciliation process
- signature of department head

***Be sure your PCI documentation is updated to reflect new equipment and processes.** The Stand-alone desk terminals use Elavon's Safe-T Solo solution to encrypt data and allow for processing via Ethernet.

Each merchant must have a detailed description of the processes in place for their card activity. These procedures are not only necessary for us to gain an understanding of your CHD environment, but are needed so you, in the department, have an understanding of the process and ensure all necessary safeguards are in place for safe cash handling and security. They are also essential to meet PCI documentation requirements.

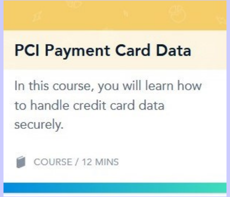
Please submit your updated documentation by Friday, May 17th to: bursar@unl.edu

Payment Card Data Security Training

All personnel involved with cardholder data need to annually complete card data security training. The course titled **PCI Payment Card Data** is available via the Bridge LMS Training & Development tile in Firefly, to satisfy this requirement.

To locate the course in Firefly - select the Bridge LMS tile in the Self Service section. Click the Search bar and search "PCI" to pull up the **PCI Payment Card Data** course (12 mins).

Since your department knows which individuals are involved with card processing, the monitoring and documentation of this training is the department's responsibility.



PCI Payment Card Data

In this course, you will learn how to handle credit card data securely.

COURSE / 12 MINS

University of Nebraska-Lincoln

Information Technology Services (ITS)
Chris Cashmere ccashmere@nebraska.edu

Office of the Bursar
Lisa Hilzer lhilzer3@unl.edu
Jennifer Hellwege jhellwege2@unl.edu

University of Nebraska Lincoln

The PCI Compliance Team is a collaboration between Information Technology Services (ITS) and the Office of the Bursar. It is a cross-functional team responsible for administering the University of Nebraska-Lincoln payment card policies and procedures, monitoring payment card activity, and educating merchants.

COMING SOON: PCI Compliance Self-Assessment Questionnaires (SAQ)

One of the most important merchant responsibilities for maintaining PCI compliance is completing and submitting the annual Self-Assessment Questionnaire (SAQ). To meet this responsibility, each University merchant account is required to submit a SAQ thru the Elavon PCI Compliance Manager portal. If your department uses only Stand-alone terminals, the PCI Team will collect the necessary information for the SAQ and submit the SAQ on your behalf as a single group. For merchants with substantial changes from last year, unique operations, or non-Stand-alone terminal setups (such as eCommerce stores or Point of Sale Registers) we will schedule Zoom meetings, primarily in June, with those merchants to aid with completing and submitting the required SAQ.

ATTN New Merchants: If your merchant account is new this year, you may have done a mid-year SAQ. We will still ask you to repeat the SAQ process in June to align your compliance reporting with the rest of the University merchants.

We will continue with the goal of completing our compliance efforts by June 30th of each year. This is consistent with efforts on the other campuses as well.

NEW PCI DSS v4.0 Requirements (part of the SAQ process)

PCI DSS (Payment Card Industry Data Security Standard) version 4.0 went into effect March 31, 2024 and is now the current security standard. It aims to better support businesses in their efforts to secure payment card data and improve security measures to protect against potential risks. PCI DSS compliance is mandatory for any business that accepts credit and debit cards.

For **Stand-alone terminals** and **POS** merchants, nothing is needed at this time.

For **eCommerce (SAQ-A)** merchants, one of the new requirements is to provide an Attestation of Scan Compliance each quarter for the eCommerce site. The first quarterly scan will be needed before or during your annual SAQ meeting in June (referenced in above section).

- For eCommerce SAQ-A merchants who **completely outsource** their eCommerce site and services to a third party, the merchant must gather the needed scan attestation directly from their provider. A scan will be needed quarterly going forward.

  ⇒ **ACTION:** Determine who in the department will reach out to the eCommerce provider, and start to have a conversation about getting their Attestation of Scan Compliance.

- For eCommerce SAQ-A merchants who **manage their own site or the University locally hosts their site**, ITS can provide PCI scanning and attestation services. ITS can provide a PCI compliant quarterly scan service and acquire the needed attestation through our PCI ASV scanning vendor, Tenable. As of now, this scan and attestation is no charge for University merchants. If site fixes are needed, it will be the merchants responsibility to bring the site up to standards.

  ⇒ **ACTION:** Email Chris Cashmere to identify your site(s) and run preliminary scans. Some sites may need updates or other work done to achieve a passing scan, so we'll want to start as soon as possible. Chris will need your Merchant ID (MID), Merchant Name, and URL/site information.

If you have questions, email Chris Cashmere and Lisa Hilzer so that we can steer you in the right direction.