Payment Cards Processing at UNL

University of Nebraska —Lincoln
Bursar’s Office

Continuum Assisting UNL’s Compliance Efforts

UNL has hired Continuum Security Solutions out of Omaha to assist in our compliance efforts this year. They will be holding three days of training to start their engagement.

ALL MERCHANTS are strongly encouraged to attend any and all of the Training
Wednesday - Friday February 4th, 5th, & 6th

The training will be broken down into sessions. We urge you to attend at least the training which is applicable to your merchant account and role within your department. For your convenience, we also hope to offer the sessions via AdobeConnect.

DAY ONE – Wednesday, February 4th @ East Campus Union, Great Plains Room (2nd floor)
The first day is more of an overall PCI review and is applicable to anyone involved in credit card processing. Please take advantage of this session and have as many associates attend this day as possible. The day’s schedule is as follows:

9:00 — 11:00 PCI DSS v3.0 Overview
11:00 — 12:00 Scoping/Network Segmentation Discussion
1:00 — 2:30 Scoping Exercise / Document Review
2:45 — 4:30 SAQ Walkthrough (w/o getting into details)

Target Audience: 1) Network Administrators, 2) Business Office Staff that understand contracts for third party payment processors and are involved in any payment card processing policies and procedures for the department, 3) Analysts who work with vulnerability scans, 4) Technical Support for systems which cardholder data resides or flows through, 5) System Administrators for applications relevant to card processing, and 6) Information Technology Services (ITS) Security Team.

DAY TWO & THREE – Thursday & Friday, February 5th & 6th
The second and third days are broken out by PCI Requirement so you can attend only sessions applicable to your merchant account.

Thursday, February 5th @ East Campus Union, Great Plains Room (2nd floor)
8:30 — 12:00 PCI Requirements 1, 2, & 3
Install & maintain a firewall configuration to protect cardholder data, Do not use vendor-supplied defaults for system passwords and other security parameters, Protect stored cardholder data.

Target Audience: 1) Network Administrators (firewalls, routers, switches, etc), 2) Technical Support for systems which cardholder data resides or flows through, 3) System Administrators for applications relevant to card processing, & 4) ITS Security Team.
Continuum Assisting UNL’s Compliance Efforts (Continued)

Thursday, February 5th (Continued)
1:00 — 2:30  PCI Requirements 3 & 4 
Protect stored cardholder data, Encrypt transmission of cardholder data across open, public networks
Target Audience: 1) Technical Support for systems which cardholder data resides or flows through, 2) System Administrators for applications relevant to card processing, and 3) ITS Security Team.

2:45 — 4:00  PCI Requirements 5 & 6 
Protect all systems against malware and regularly update anti-virus software or programs, Develop and maintain secure systems and applications
Target Audience: 1) Technical Support for systems which cardholder data resides or flows through, 2) System Administrators for applications relevant to card processing, and 3) ITS Security Team.

Friday, February 6th @ East Campus Union, Great Plains Room (2nd floor)
9:00 — 12:30  PCI Requirements 7, 9 & 12 
Restrict access to cardholder data by business need to know, Restrict physical access to system components, Maintain a policy that addresses information security for all personnel
Target Audience: 1) Business Office Staff that understand contracts for third party payment processors and are involved in the payment card processing policies and procedures for the department, 2) Technical Support for systems which cardholder data resides or flows through, and 3) ITS Security Team.

1:30 — 3:30  PCI Requirements 8 & 10 
Identify and authenticate access to system components, Track and monitor all access to network resources and cardholder data
Target Audience: 1) Technical Support for systems which cardholder data resides or flows through, 2) System Administrators for applications relevant to card processing, and 3) ITS Security Team.

3:45 — 4:30  PCI Requirement 11 
Regularly test security systems and processes
Target Audience: 1) Analysts who work with vulnerability scans, and 2) ITS Security Team.