Additional Training a Must for ALL in V3.0

There are specific training requirements in V3.0 which must be adhered to by all parties handling cardholder data. Since only your department knows which individuals are involved in card processing, the monitoring of this training will be the department’s responsibility.

Cash Handling Training
All personnel connected in any way with cash handling, including payment card transactions, must review cash handling policies & procedures on a regular basis. A review should occur at least annually and documentation of this review should be retained within the department. Cash handling policies & procedures training is available at: http://bursar.unl.edu/cash-handling-policies-procedures

Security Awareness Training –Requirement 12.6
All personnel connected in any way with cardholder data need to annually complete security awareness training at http://its.unl.edu/security/security-awareness-training.

Departments can contact Cheryl O’Dell with a listing of employees who need to complete the training if you’d like to request access as a group instead of individual requests. Cheryl can also provide reporting to departments so they can ensure all employees have complied with this requirement.

Device Tampering Training –Requirement 9.9
All personnel must be trained to protect devices which capture payment card data through physical interaction (i.e. swipe, dip, or wave) with a payment card. Personnel must be trained to be aware of attempted tampering or replacement of devices, and terminals must periodically be inspected to look for tampering and substitution.

Two resources that we’ve found to be helpful are:


Either of these could be used for training within departments and, again, the department must document all who need training have received it.
Design of eCommerce Sites is Crucial to Managing Compliance

If you have an eCommerce site, designing your site with the intent to reduce your PCI scope will greatly help you manage your PCI compliance responsibilities.

Redirects
Under Version 3.0, the site that transfers your customers to your card processor, or the pay now button, is in scope for PCI. This is referred to as a redirect.

If you have multiple sites redirecting to, for example Payflow Link, then each individual site is in scope for PCI. A site design which has only one place or page doing the redirect for various purchase options can reduce your PCI scope. That should always be our goal when we develop our merchant websites. Consolidate all your eCommerce to one server whenever possible. Then only that server will be in scope, and your compliance efforts can be minimized.

ITS is working on a checklist for guidance on the security of redirects. There are a number of items that must be looked at to bring these sites into compliance under V3.0. They can be found in SAQ A-EP.

Charging a Fee for Payment by Card
Payment card regulations make it very difficult to charge an additional fee (surcharge) when a customer pays their account using a credit/debit card. There are notification requirements, calculation requirements, getting acknowledgement from the customer requirements, among others. Rarely is the amount collected as a fee for presentment of a credit/debit card going to outweigh the cost of fulfilling the notification requirements. A better approach is to build into the price of your product an amount to help offset the fees.

The exception to this is for payments on a UNL Student Account using a credit card which is a convenience fee. It is a unique arrangement with the company which processes all of our online payments and is paid directly to them.

You can, however, charge a fee for making payment at the ‘door’ of an event. This would be a late registration fee and must be applicable to all payment types accepted. It is not the customer’s choice of payment method that creates the fee, but instead the timing of their payment.

Sending Cardholder Data Among Offices
If you are collecting cardholder data (CHD) in one location and another location is then processing the transaction, the method of delivery of the data must be considered in your compliance efforts.

Per our QSA, “The transmission of the cardholder data has to be sent via a traceable method. That can mean that you use a FedEx or USPS tracking number, or it can simply mean that there is a formal process for tracking how many sheets were collected, who is transporting them, and then formally acknowledging their receipt at their final destination.”

In other words if you are mailing data between offices, a formal process must be in place to track the sending, receiving, processing and storing of the CHD.