Did you know?
Sodexo now has a web site that can be used to pay for catering. Please do not send p-card data to Sodexo via email or interoffice mail. Their new catering site can be accessed through their current site and can also be accessed directly at the following web address:

https://binghamton.catertrax.com/

Procurement Cards and the PCI DSS
For those employees on campus who have a procurement card (p-card), the first thing to keep in mind is that your p-card is no different than any other Visa credit card. You should be equally vigilant, if not more so, about the security of your p-card as any other credit card in your wallet. Banks and the merchants they have authorized to accept credit cards are responsible for the requirements of the PCI DSS. It is through this compliance that fraud protection is made possible for all consumers that use credit cards. When using a p-card, as a consumer you are not responsible for the PCI DSS or the consequences of potentially fraudulent activity.

However, a unique circumstance occurs when a p-card is used to pay for goods or services from another campus department. In that specific scenario, Binghamton University is both the consumer and the merchant. So, BU has responsibility for PCI DSS compliance for this particular credit card transaction. Another thing that is unique about this transaction is that often times the p-card user knows the employee from the merchant department to whom payment is being made. Our campus merchant departments know to reject a credit card number received by email. But, when they know the sender, following proper procedure is not always easy.

The unique set of circumstances described above has resulted in the following practices taking place:

- P-card numbers have been emailed from one campus department to another, and
- Cardholder data from p-cards has been written down and sent to another campus department using interoffice mail.

Neither of these practices are secure and both violate our campus policies.

How can P-card holders help?
First, never send your cardholder data in an email to anyone, ever. This includes other BU departments. Not only is this an unnecessary risk, but it is also a violation of campus policies. Next, avoid using interoffice mail for this purpose. But if you must, then please treat credit card data the same as cash. Use a locking bank bag. A better alternative would be to pay using the merchant department’s web site. Using an eCommerce solution (such as the one mentioned on the right), or the telephone are both preferred methods of communicating your credit card number to another campus department or any other vendor. Finally, please safeguard your p-card the way you would with any of your personal credit cards.
Third Party Contracts Revisited

In the December issue two important requirements associated with third party contracts were discussed. First, PCI liability limiting language is required in each contract that BU has with a third party service provider. Second, we need an Attestation of Compliance (AOC) annually from each one of our vendors. These can be found as components of Requirement 12 of the PCI DSS.

Requirement 12 also mentions three additional items associated with third party contracts:
1. A list of Service Providers must be maintained. This is done campus wide at Revenue Accounting. However, a separate list should be maintained by each department that has more than one vendor.
2. A formal process must exist for engaging service providers. This should already be in place via campus RFP procedures.
3. Documentation should be maintained that shows which party is responsible for what portion of the PCI DSS. Some contracts already show what the vendor is taking responsibility for. The BU department should document their own responsibilities in their credit card processing written procedures.

PCI DSS Compliance Training 2015

All training notifications have been sent to required participants. Thank you to all who have already completed the training module! If you have not done so, please login at www.wecomply.com and complete the module as soon as possible. Supervisors will be informed of all staff who have not completed the PCI DSS training module by March 2, 2015. Failure to complete training is considered non-compliance with the PCI DSS. (See below)

CampusGuard Portal

Currently, we use the CampusGuard Portal to fill out our Self-Assessment Questionnaires (SAQ). In addition, we would like to make further use of the portal to store all of our documents that are necessary for compliance. Examples of documents include, department procedures, list of third party vendors, and AOCs. Steve Duseau will be in touch with each department regarding how to access the portal.

Best Practices

- Never e-mail credit card information or store credit card numbers in any database or spreadsheet.
- Truncate all but the last four digits of the card number. Keep all credit card documentation locked. Destroy it when no longer needed.
- Limit access to cardholder information to only those employees with a legitimate need to know. Also, segregate duties so that the person performing reconciliation isn’t involved in processing credit card sales or refunds.
- Encourage a proactive focus on security, rather than just a focus on compliance. A merchant can be compliant but not fully secure.
- All in-person payment card transactions must have the actual card present.

Periodic Reviews and Audits

The Revenue Accounting Office will regularly review the SAQs on the CampusGuard Portal, along with all attestations, training, department procedures, controls and documentation within the CDE (Cardholder Data Environment). Additional information and follow-up interviews may be requested and visits to merchant locations may take place when necessary. The intention of these activities is to reduce the University’s risk by ensuring that merchants comply with the PCI DSS. Failure to cooperate with such activities and maintain compliance may result in your department’s merchant account being revoked.