What’s happening on campus?

CampusGuard Report from the July Visit

This past July 25th and 26th our QSA from CampusGuard visited our campus to assess our PCI Compliance. The report containing his findings was released two weeks ago. All campus merchant departments are considered to be compliant with respect to their business practices. This of course assumes that all departments follow their PCI DSS related policies and procedures each business day. It further assumes that all department employees are appropriately trained. Unfortunately, we know this is not the case, as there are still 40 employees campus wide that have not completed the training module.

In addition, there are specific pieces of our IT infrastructure that are currently not in compliance with the PCI DSS. So, four of our campus merchant departments that rely on IT resources for their payment processing are not yet compliant. It is for this reason that CampusGuard strongly recommends the use of point to point encryption (P2PE). The use of a PCI validated P2PE solution would mean that our IT infrastructure would not handle any credit card numbers and therefore, it would be considered out of scope. We are very close to having P2PE in place. The difficulty has always been that our vendors of point of sale software must integrate with a P2PE solution provider. In some cases, campus merchants are switching their software to a vendor that has P2PE. But, both vendor changes and software integrations take time.

RFP 16/17/004

The evaluation phase of the e-commerce RFP is nearing completion and we should have a vendor chosen very soon. More details should be available in the December newsletter.

Did you know?

October is Cyber Security awareness month.
Among the statistics for 2016, over three million records are compromised every day which comes out to about 35 records per second.
Outstanding Compliance Issues

1. Annual Training - there are still 40 employees that need to complete training. Please ensure that everyone in your department is trained. Reminders will be sent out and continue until training is completed.

2. Many Attestations of Compliance (AOCs) from third parties have expired, and a few have never been obtained. If a third party collects payments on our behalf, we must ensure that company is PCI compliant. In addition, all contracts with third parties must contain PCI language. The proper language will make it easier to obtain the annual AOC.

If you have questions, please contact Steve Duseau. sduseau@binghamton.edu

Data Security Breach at the University of Central Florida

In February of this year, the University of Central Florida, located in Orlando, suffered a data breach. UCF is a public university with an enrollment that exceeds 60,000. Fortunately, credit card numbers were not lost in the breach. But, student records along with faculty and staff information was affected. Names, addresses, university IDs, and social security numbers were among the records that were compromised.

Third Party Service Providers

If a business provides remote IT systems support to its customers, then that business is responsible for maintaining unassailable standards of security. Such businesses must agree in their contracts with their customers that the business will indemnify the customer from any breach resulting from the provider’s side. When IT systems provided to customers include a credit card accepting component, then the customers must be provided an AOC based upon ‘SAQ-D for Service Providers’. Anytime this AOC is provided, then the service providing company is absolutely responsible for operating security best practices determined by the PCI DSS (see www.pcisecuritystandards.org/documents/AOC_SAQ_D_v3_Service%20Provider.docx) Conversely, if a business is a PCI Merchant or Payment Provider then that entity must make sure that its IT Service Providers have provided an appropriate indemnification and AOC.

For BU, we must not put our ITS department in a position that causes it to act as a PCI service provider to campus merchants. Also, our campus merchants must hold the third party service providers that they do work with accountable for PCI compliance.