What’s happening on campus?

2015 CampusGuard Visit

Ed Ko, our Qualified Security Assessor (QSA), from CampusGuard visited BU August 3rd-5th. During his visit, Ed was very impressed with the great progress we have made towards becoming compliant. In the weeks to come, Ed will send us his report and we will pass it along to the campus merchant departments. The report will outline what each department must do to become compliant. Generally speaking, it just comes down to having the proper documentation in place.

Documentation

Almost all departments already have their documentation on the shared drive so that it can be easily reviewed. Please save copies of your documentation to the shared drive if you have not already done so. If your department made its documentation available for Ed’s visit, then his findings were that minor updates needed to be made and, in some cases, missing documents needed to be added. For the most part, the missing documents were the training acknowledgement, the visitor log and the terminal inspection log. Please note, the terminal inspection log does not apply to every department, only if you have credit card terminals such as the Vx510 or Vx680. Also, the terminal inspection log is a new requirement under version 3.1 of the DSS. So, it is understandable that no one had such a log. More about logs on page two. The best way to ensure that your department’s documentation is complete is to run the checklist available on the shared drive. Contact Steve Duseau if you’d like the checklist emailed to you or if you cannot easily access the shared drive.

SAQs

Another important part of our compliance documentation is the Self Assessment Questionnaire (SAQ). I’m pleased to say that these are all complete by each department. However, they are not all accurate. Steve Duseau will be reaching out to certain departments to help you achieve accuracy. If you do not hear from Steve in this regard, your SAQ is both complete and accurate at this time.

Did you know?

There is a wealth of information available on the shared drive to assist you in achieving compliance for your department. If you are having any difficulty accessing the shared drive, please contact Steve Duseau immediately.

Remember to keep terminal inspection logs for each terminal. Make the appropriate log entry prior to each day’s use of the corresponding terminal.
Training Acknowledgement

Thank you to everyone for completing the annual training this year. Remember, student employees who will begin working for your department this fall need to be trained within one week of starting work. We do need to document the fact that our employees who handle CHD have received the annual PCI training. This can be accomplished using the training acknowledgement document which can, of course, be found on the shared drive. Please obtain the document from the “Adopt and Use” folder and modify it as needed so that it fits the specifics of your department. Then have your employees sign and date the acknowledgement.

The Shared Drive

Hopefully the need to access the shared drive is abundantly clear to everyone. If you cannot access it, please inform Steve Duseau immediately. It’s location: \firestone\bgmshare\PCI DSS Documentation

Documentation Reminder

Three campus merchant departments still have not saved ANY documentation to the shared drive. A handful of others still need to update their documentation per Ed’s suggestions at the meeting earlier this month. Please get all proper documentation on to the shared drive! The deadline has passed.

Keeping Logs

On page one, everyone was reminded of the need to keep logs. The first log everyone should keep is a Visitor’s Log. Any visitor who enters your Cardholder Data Environment (CDE) should be logged in and out so that you have a record of who was there and when. This log should be filled out by department staff and not by the visitor. Also, no visitor should be able to view the log such that he or she can see the other names contained on it. Departments should also document the need for this log in their PCI related policies and procedures. It is also a good idea to clearly define your department’s CDE in your policies and procedures document. Define both its physical location and the days and times it is operational. A well defined CDE means that it is feasible that there will rarely be a need to log a visitor in. It is also permissible to prohibit visitors to your CDE while it is operational.

The second log we must now keep is the terminal inspection log. This log is a new PCI DSS v3.1 requirement. (Req. 9.9) This only applies to the six campus merchant departments that actually have credit card swipe terminals. A log sheet should be created for each terminal that your department has. An inspection should be performed and a log entry made for each business day that terminal will be used prior to the first use of the day. If a terminal will not be used, no log entry is required that day.

All logs should be three hole punched and stored in a binder. Additionally when a log sheet becomes full of entries, you can scan it and save it to the sub folder labelled “Logs” within your department’s shared drive folder. Generic versions of the logs are available on the shared drive in the “Adopt and Use” folder.