

PCI DSS SELF-ASSESSMENTS OR QUESTIONNAIRES

The Payment Card Industry Data Security Standards Council has put together Questionnaires for merchants to self-assess their compliance. The questionnaire you are required to complete depends on what equipment or software, or other processing method you use to process payment cards in your department.

The following are links and hints to select and complete the correct questionnaire

Questionnaire A

- Fill out Questionnaire A if you meet the following qualifications:
 - You utilize a system where the payment card data and processing are totally hosted by a third party
 - The application is not being used as a POS, where employees are entering mail/phone orders via the web.
- A NEW Questionnaire must be completed each year. If you have not done a questionnaire yet, create a new one.
- The goal is to be able to answer “yes” to all of the questions.
- **Questionnaire A** is in .pdf form and must be submitted via fax or sent directly to OTO/FREH.

Questionnaire B

- Fill out Questionnaire B if you meet the following qualifications:
 - You use a stand alone, dial-up terminal which does NOT connect to the internet or any other system within the merchant environment;
 - You do not store cardholder data in electronic format; **and**
 - You store cardholder data in paper reports or copies of paper receipts which are not received electronically.
- A NEW Questionnaire must be completed each year. If you have not done a questionnaire yet, create a new one.
- The goal is to be able to answer “yes” to all of the questions.
- **Questionnaire B** is in .pdf form and must be submitted via fax or sent directly to OTO/FREH.

Questionnaire C

- Fill out Questionnaire C if you meet the following qualifications:
 - You use a standalone terminal that has a direct internet connection through the University network;
 - You use a payment application system that utilizes the internet or public network connection (i.e. a point of sale register);
 - The payment application system/Internet device is not connected to any other system within the merchant environment;
 - You store cardholder data, such data is only in paper reports or copies of paper receipts and is not received electronically; **and**
 - Your payment application software vendor uses secure techniques to provide remote support to your payment application system.
- **Questionnaire C** is in .pdf form and must be submitted via fax or sent directly to OTO/FREH.
- The goal is to be able to answer “yes” to all of the questions.
- You may need the assistance of your IT support to answer some of the more technical questions.

Questionnaire D

- Fill out Questionnaire D if you meet the following qualifications:
 - You use a Third Party Payment Application that is installed on a campus server;
 - You use a campus server for E-Commerce, and are not utilizing Touchnet to collect sensitive cardholder data;
 - The qualifications for Questionnaire B and C do not completely apply to your processing method.
- **Questionnaire D** is in .pdf form and must be submitted via fax or sent directly to OTO/FREH.
- The goal is to be able to answer “yes” to all of the questions.
- You may need the assistance of your IT support and Vendor representative to answer some of the more technical questions.

Information Security

- Firewalls (internet terminals)
- Information Storage
- Payment Card Industry Data Security Standard
- Securing the network
- University Information Technology Resource Security Policy
- Security checklist for Third Party Vendor Implementation