Payment Card Information Self-Assessment Questionnaire Checklist

Due: November 9, 2018

- ☐ Schedule an initial consultation appointment with the Payment Card Coordinator, Contact: merchantservices@ucsc.edu

Note: Please, do not begin filling your SAQ out in Coalfire.one at this time.

We are moving to a new SAQ platform. Please focus on preparing the documentation below and await information about portal access.

Click each item to download a general template. Templates for these items can also be found on the Merchant Services webpage. Full descriptions of each item on this list can be found on pages two and three of this document.

Update, or prepare the following required documentation:

- ☐ Departmental Credit Card Security Policy
- ☐ Incident Response Plan
- ☐ Training & Policy Certification
- ☐ Contract information for Credit Card processor and involved third parties:
  - E.g. Payment processor (Stripe, Auth.net), Integration software (iModules, etc.)
- ☐ Service Provider List
- ☐ Access control list
- ☐ Equipment Tracking List
- ☐ Terminal Tamper Inspection Checklist
- ☐ Photos of Credit Card Terminals:
  - Front and back, clearly capturing serial number information
  - Can be gathered in a word document or as individual files
- ☐ Attestation of Ecommerce Only Processing (Only E-Commerce Merchants)
  - For departments with only ecommerce solution.
- ☐ Submit SAQ(s) in DigiTrust Portal:
  - Access to this system will be sent out as soon as possible

Payment Card Information Self-Assessment Questionnaire Checklist

Due: November 9, 2018

Document Descriptions:

Departmental Credit Card Security Policy: This document outlines the policies and procedures put into place by your department to protect cardholder data. This is often one of the more time consuming aspects of establishing your PCI compliance documentation, so plan ahead and give yourself time to complete it. Not all aspects of the template may apply to your current operation. You are welcome to delete sections that do not apply to your organization. If you are not comfortable doing so, please contact merchantservices@ucsc.edu.

Incident Response Plan: This document prepares your unit for efficient action and communication in the event of a suspected or confirmed breach of a physical, or digital environment. Most critically, it should contain the exact steps of what to do under breach circumstances, as well as contact information of the person in the unit/division that will report the breach to relevant parties. Typically this is the PCI Coordinator for the unit reporting to the Payment Card Coordinator by phone and by emailing merchantservices@ucsc.edu.

Training & Policy Certification: This document is signed by the departmental PCI Coordinator and Department Head to certify that they understand that critical aspects of UCSC's PCI and Merchant policies and procedures are to be followed. Full details are available in the document.

Service Provider List: This document lists all service providers, including a description of service provided. Depending on the complexity of your environment, this could be as few as one service provider or more than three. Generally our acquiring bank is not listed (Bank of America). Please list contact information for each party so that they can be reached in the event of a breach or other emergency.

Access Control List: Documentation of positions that have access to your credit card environment and their access level. This list enables your organization to know who should and should not be touching credit cards and management environments so that if unusual activity occurs you know who is cleared to be involved and who isn't.

Contract information for your Credit Card Vendor and/or Service Providers: All parties engaging in business with UCSC should be contracted, and contracts with companies dealing with Card Data must be on file in order for UCSC to ensure that the third party is compliant with PCI DSS regulations. If a party is handling card data directly (Stripe, Authorize.net, etc.) an up-to-date QSA signed SAQ should be on file. These parties must also agree to UC's Security Appendix DS. You can request this information from your Service Providers, Procurement, or ask merchantservices@ucsc.edu for assistance in obtaining contract information.

Payment Card Information Self-Assessment Questionnaire Checklist

Due: November 9, 2018

Equipment Tracking, Photos and Movement List: List of all credit card terminals, models, serial numbers, their physical locations, and pictures of each terminal, front and back. This information is critical to provide baseline information for tamper checks and equipment tracking. Depending on the number of terminals and frequency of their movement, different tracking sheets and methods can be used. Tracking of terminal movement and logging of employees moving them deters improper access and creates an access log for audit in the event of a breach or audit.

Terminal Tamper Inspection Log: Proof that terminals are being inspected on a regular basis.

Attestation of Ecommerce only Processing: For E-commerce only merchants, a statement attesting that no physical credit card terminals are being used can be submitted instead of a tracking list. This statement should be signed by the departmental PCI Coordinator and Department Head.

When is my SAQ Due?

SAQ's must be submitted with supporting evidence for each question by **November 9, 2018**.

How do I get help?

If you need assistance with any aspects of your SAQ please email merchantservices@ucsc.edu.

Where do I complete my SAQ?

We are currently waiting for Coalfire to provide us access to the new DigiTrust SAQ Portal. More information to come on how to access and use the new interface.