PCI Compliance at the Department Level

Finance Area:

Vice President for Finance

Responsible or Contact Office/Role:

Financial Reporting & Operations (Payment Card Services)

Last Review Date:

October 1, 2018

Purpose:

This procedure covers the steps a unit will follow in order to fulfill the annual requirement for PCI Compliance as mandated by the Card Brands (VISA, MasterCard, Discover and American Express) and administered though the PCI DSS (Payment Card Industry – Data Security Standards) and the PCI Council.

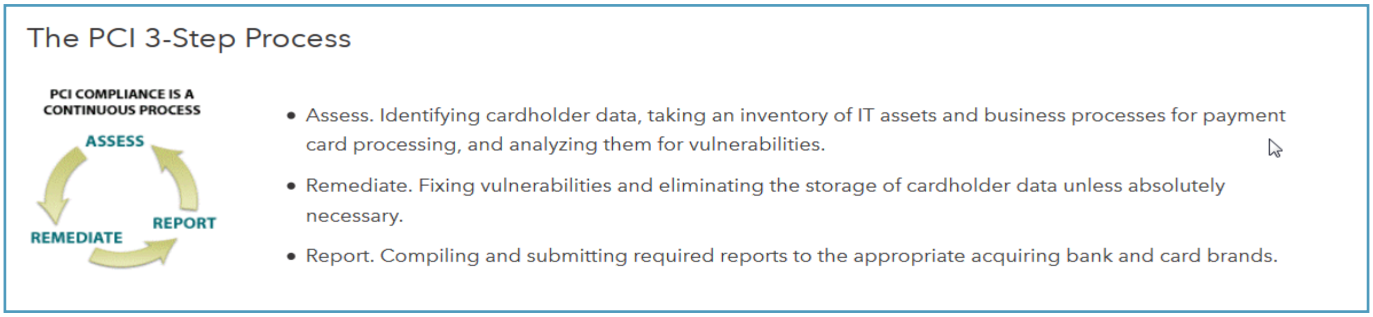
Procedures:

- **Assign a PCI Coordinator**
  - who will serve as the primary point of contact between the unit and University and is responsible for Documentation, the Security Review, and Third-party documentation - PCI Coordinator
  - who completes a one-time, classroom training through FOC (Finance Outreach and Compliance).

- **The Coordinator**
  - Provides Front-Line staff Training, for new staff and annually for all staff which includes anyone who is in direct contact with customers or has access to cardholder data or reconciliations.
- **InfoSec** - annual Information Technology Security Awareness tutorial see policy IRM-002 Acceptable Use of the University's Information Technology Resources.
- **Documentation**
  - Distributes and collects Confidentiality Agreements via DocuSign and the
  - Completes and submit Desktop procedures for each payment card process (swipe or web), to be reviewed annually for changes.
  - Provide Equipment Inventory form (Requirement 9.9.1 – *Maintain an up-to-date list of devices…) form for desktop swipe or cellular based terminals and Fax Machines, see Fax Machines below).*
  - Oversees the annual SAQs (Self-Assessment Questionnaire). A unit may be required to complete a separate SAQ for each process, e.g. an SAQ A for web and an SAQ B for swipe (desktop or cellular). Submission may include;
    - Education of the Signatory on PCI and SAQ compliance and liability obligations, signs the Attestation of Compliance,
    - Complete and submit the UVA PCI Supplement,

- **Security Review** with the local IT professional. For additional guidance contact Payment Card Services and InfoSec for assistance.

- **Website** A review of the website
    - What server is the website on and who manages the server? (If your website sits on a UVA server, chances are that the patches or required updates (SSL) have NOT been applied.
    - Secure your Website. If passing data into the payment page or receiving a response back, the entire website must be reside on a PCI compliant platform (AWS, Salesforce, AZURE etc).
    - Secure Your Payment page. If the department is NOT passing data into the payment page or receiving data from the vendor (usually those using EPAY exclusively) then a “Landing Page” is required to comply with our Processor and the Card Brand rules.
    - See Requirement 6.6 for Public-facing web applications in the PCI Standards.
    - Review PCI Guidance to Safe payment processing.



The PCI 3-Step Process

- Assess. Identifying cardholder data, taking an inventory of IT assets and business processes for payment card processing, and analyzing them for vulnerabilities.
- Remediate. Fixing vulnerabilities and eliminating the storage of cardholder data unless absolutely necessary.
- Report. Compiling and submitting required reports to the appropriate acquiring bank and card brands.

- **Swipe or Cellular Terminal PCI** and our Processor have control over the devices that they provide to us. ITS Enterprise Infrastructure has control over the connections that these devices use at the University. See https://www.pcisecuritystandards.org/assessors_and_solutions/pin_transaction_devices for the current list and expiration dates.
- (Requirement 9.1.3) *Restrict physical access to wireless access points, gateways, **handheld devices**, networking/communications hardware, and telecommunication lines.* Requirements 9.9, 9.9.1, 9.9.2, 9.9.3 Protect the device, inspect and catalog.
- **Wireless access points** (Requirement 4.1.1) *“Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices to implement strong encryption for authentication and transmission.”* This requirement is especially relevant for outside vendors who are on grounds, using our wireless network for payment card processing.
- **FAX machines** (Requirement 9.5) Physically secure all media – *Verify that procedures for protecting cardholder data include controls for physically securing all media (including but not limited to computers, removable electronic media, paper receipts, paper reports and **faxes**).* See Swipe Terminal guidelines above. Fax machines should be programmed to print during business hours only and be located in a non-public area.

Third-Party Provider and POS vendor compliance review

- Properly vet any Third-Party Provider who has a role in collecting Personal or Cardholder data whether the units is receiving financial benefit or involved in the process directly or indirectly. Contact Payment Card Services and/or Information Security, Policy and Records (aka InfoSec) for assistance before contracts are signed or revenue is received.
- Provide compliance documentation (AOC if vendor processes < 300,000 total payment card transactions annually or ROC (signed by a QSA [Qualified Security Assessor] and processing > 300,000 total transactions annually) and Payment Card Flow Diagram) for all Third-Party.
- Understand and supply the cardholder data flow diagram from your third-party providers annually as part of their PCI Compliance obligations. For Nelnet/EPAY ONLY users, complete this document. See guidance from Campus Guard on

creating your own Cardholder Data Flow diagram in order to comply with Requirement 1.1.3 – “Current diagram that shows all cardholder data flows across systems and networks.” https://www.campusguard.com/public/NewsArticle-2018.07.20-DataFlowDiagrams.pdf

Other Resources

- Collab - UVA’s central online environment for teaching, learning, collaboration, and research for UVA PCI Coordinators and UVA PCI Tech (see tutorial). A resource for PCI Compliance documents and communications.
- CampusGuard, and Portal User Guide. Campus Guard is the University’s information security partner specializing in PCI DSS compliance.

Immediately notify Payment Card Services if any changes occur with staff, vendors, contracts, processes or procedures.