Payment Card Industry Data Security Standard (PCI DSS) Information

Merchant Responsibilities

- Complete the appropriate annual Self-Assessment Questionnaire and maintain compliance.
- Notify the Treasurer’s Office and your campus Chief Business Officer of any potential changes to your approved processing procedures.
- All systems that handle, process, or store credit card numbers must be registered with your campus Chief Information Officer (CIO).
- Work with your campus CIO to place PCI systems in the segmented cardholder data environment.
- Merchants may never accept or send Primary Account Numbers (PAN) by email or text message.
- Merchants may not use UT-issued or personally-owned mobile phones or devices to process credit card transactions.
- Merchants may not use personally-owned systems to process credit card transactions.
- Merchants may not use Wi-Fi to process credit card transactions.
- Any staff member processing credit card transactions must participate in annual PCI security training.
- Internal policies and procedures must be documented and maintained.
- The PCI Inventory Log must be maintained and contain:
    - Make and model of device;
    - Serial number of device;
    - Function of device;
    - Location of device;
    - Person(s) responsible for device;
    - Date of last inventory check;
    - Name of each staff member explicitly authorized to use device; and
    - Name(s) of management giving explicit authorization to use device.
- Regularly inspect POS devices for signs of tampering.
- Update credit card terminal software every 12-18 months, where applicable.
- Immediately notify the UTSA ISO and your campus CIO in the event of a suspected data breach.
    - Do not make any changes to the system(s) involved in the suspected breach.
    - Do not turn off the system(s).
- Merchants are financially responsible for costs associated with compliance, including fines, fees, and remediation expenses.

Cardholder Data Storage Requirements

- Cardholder data may not be stored on any UT system.
- Card verification code (CVC2, CVV2, CID) may not be stored under any circumstance after initial transaction approval.
- Protect cardholder data and ensure appropriate security controls.
  - Technical controls should be placed on systems that process cardholder data.
- Store media (electronic and/or paper) in locked containers and in secured areas with limited access.
- Schedule the proper disposal of cardholder data based on business, legal, and/or regulatory requirements as documented by the department.
- Destroy or securely remove all cardholder data from all media before disposal or reuse.

Links

- **PCI Compliance at UT:** http://security.tennessee.edu/pci-dss-compliance-information/
  - Training
  - Merchant Documentation Templates
  - Security Awareness Information
  - PCI Standards and Procedures for UT Merchants
  - SAQ Guides
  - Additional PCI resources
- **UT Policy Site:** http://policy.tennessee.edu/
  - Fiscal Policy FI0311 – *Credit Card Processing*
  - IT Policy IT0110 – *Acceptable Use of Information Technology Resources*
- **PCI Security Standards:** https://www.pcisecuritystandards.org
- **VISA PCI Compliance Information:** https://usa.visa.com/partner-with-us/pci-dss-compliance-information.html
- **MasterCard PCI Compliance Information:** http://www.mastercard.com/us/company/en/whatwedo/site_data_protection.html
- **Discover PCI Overview:** http://www.discovernetwork.com/merchants/data-security/index.html

Contacts

- **Treasurer's Office**
  - Alicia Reed – (865) 974-3467 – areed7@tennessee.edu
  - Tim Mapes – (865) 974-2302 – tmapes@tennessee.edu
- **UTSA Information Security Office**
  - Sandy Lindsey – (865) 974-8907 – sandy@tennessee.edu