Payment Card Industry Data Security Standard

**Introduction**
In an effort to protect credit card information from unauthorized access, disclosure and compromise, the Payment Card Industry (PCI), i.e., Visa, MasterCard, American Express, JCB and Discover, formed a security standards council that is charged with creating and maintaining mandatory standards which are designed to assist with properly securing payment card data that is processed, transmitted or stored by an organization.

**Purpose**
This document sets minimum baseline security requirements for all personnel and information systems which process, store or transmit payment card data.

**Audience**
All UTMB faculty, staff and students, who process, maintain and access payment card data, or maintain an information resource that processes, stores or transmits payment card data are required to comply with this practice standard. Any deviation (security degradation) from this standard requires approval from the Office of Information Security. Exception can be requested at [http://www.utmb.edu/infosec](http://www.utmb.edu/infosec).

**Implications**
- All data owners and system custodians who maintain information resources that store, process and transit card holder data is required to comply with the Payment Card Industry, Data Security Standard (PCI-DSS)
- The Office of Information Security shall assess PCI-DSS implemented security controls for effectiveness, and submit an attestation of PCI DSS compliance annually, to the Associate Vice President of Finance and Global Payments.

**Sensitive Digital Data Management**
UTMB Information Resource users are required to protect “Sensitive Digital Data” in accordance with UTMB Practice Standard 1.2.10 – Managing Sensitive Digital Data.

Sensitive Digital Data, as defined by UTS 165, includes social security numbers, Protected Health Information (PHI), Sensitive Research Data, digital Data associated with an individual and/or digital Data protected by law. Sensitive digital Data must be secured and protected while at rest (electronic storage on a hard drive, digital or optical media), mobile (laptop, PDA or flash drive) and in transit (via email or the Internet).
Payment Card Industry, Data Security Standard, continued

**Practice Standards**

**ADMINISTRATIVE REQUIREMENTS** – Departments and personnel who process payment card data shall adhere to the following requirements:

- Only departments who have a UTMB merchant ID through Global Payments are authorized to collect, process, store, or transmit payment card data.
- Departments will not store any of the following cardholder information (even if encrypted):
  - Full Magnetic Stripe
  - CAV2/CVC2/CVV2/CID
  - PIN/PIN Block
  - Full 16 Digit Personal Account Number (PAN)
- Departments may store the following cardholder’s information if a business need exists:
  - PAN’s, as long as it’s rendered unreadable through truncation
  - Cardholders name
  - Service code
  - Expiration date
- Limit the storage of payment card data to the department’s data retention schedule. Unnecessary stored data will be purged at least quarterly.
- Payment card data shall only be stored, processed or transmitted from institutional systems that are secured in accordance with this practice standard. Payment card data shall not be stored on any personally owned device, desktop computers, to include a UTMB owned desktops, or any portable computing device. Additionally, Payment card data shall not be copied to, or stored on any type of removable media, i.e., CD-ROM, DVD’s, flash drives, etc., unless it is a integrated component of an institutional system, i.e., tape backup.
- When transmitting payment card data over an open public network, i.e., the internet. It must be secured using a minimum of 128 bit encryption.
- Payment card data shall not be transmitted using end-user messaging technologies. i.e., email (even if encrypted).
- Limit access to payment card data to personnel whose job duties require such access.
- All users accessing payment card data shall have a user account created and managed using practice standard 1.2.1, Account Management.
- To minimize the risk of malicious compromises from internal sources, hiring authorities, working in conjunction with the Department of Human Resources, shall screen potential personnel (to include contractors) prior to hire. Example screening includes previous employment history, criminal record, credit history, and reference checks.
Payment Card Industry, Data Security Standard, *continued*

### Practice Standards (con’t)

**CUSTODIAL REQUIREMENTS** – System custodians responsible for information resources that process, store and/or transmit payment card data are required to adhere to the following requirements:

- Secure all information resources in accordance with practice standard 1.1.5, Platform Hardening.
- Payment card data must be encrypted when transmitting over an open public network. i.e., the Internet. Transportation protocols, including Transport Layer Security (TLS) and Secure Socket Layer (SSL), shall be configured using a minimum of 128 bit encryption.
- Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Critical patches shall be deployed within a month of release.
- All software applications (internal and external, and including web-based administrative access) shall be developed in accordance with the Payment Card Industry, Data Security Standard (PCI DSS) and based on industry best practices. Information security shall be incorporated throughout the software development life cycle.
- All changes to information resources shall be approved and documented in accordance with practice standard 1.3.1, Change Management.
- Physically secure all information resources in accordance with practice standard 1.2.6, Physical Access.
- Backup Information resources in accordance practice standard 1.3.2, Backup/Recovery.
- Deploy file integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files or content files. The software will be configured to perform critical file comparisons at least weekly.
- Enable automated audit trails so that the following events can be reconstructed:
  - all individual user accesses to cardholder data
  - all actions taken by any individual with root or administrative privileges
  - access to all audit trails
  - invalid logical access attempts
  - use of identification and authentication mechanisms
  - initialization of the audit logs
  - creation and deletion of system-level objects
Payment Card Industry, Data Security Standard, continued

Practice Standards (con’t)

- Record audit trail entries for all system components for each event, including at a minimum:
  - user identification
  - type of event
  - date and time
  - success or failure indication
  - origination of event
  - identity or name of affected data
  - system component or resource
- Using time synchronization technology, synchronize all critical system clocks and times
- Secure audit trails so they cannot be altered

NETWORK AND SECURITY REQUIREMENTS – The Information Services, Network and Security Department shall adhere to the following requirements.

- Assist custodians in configuring systems to transmit security events and audit logs to the enterprise security information manager.
- Review logs for all system components related to security functions at least daily.
- Retain audit trail history for at least one year; at least three months of history must be immediately available for analysis.
- Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis.
- Perform internal and external network vulnerability scans at least quarterly and after any significant change in the network.
- Perform external and internal penetration testing, including network- and application-layer penetration tests, at least annually and after any significant infrastructure or application upgrade or modification.
- Use network intrusion detection systems and/or intrusion prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. IDS/IPS engines, baselines, and signatures must be kept up to date.
Payment Card Industry, Data Security Standard, continued

Practice Standards (con’t)

INFORMATION SECURITY OFFICER REQUIREMENTS – The Information Security Officer shall adhere to the following requirements.

- Establish, publish, maintain, and disseminate a security policy that addresses all PCI DSS requirements, including an annual process for identifying vulnerabilities and formally assessing risks, and includes a review at least once a year and when the environment changes.
- Engage an Approved Scanning Vendor (ASV) to perform quarterly external vulnerability scans.
- Develop daily operational security procedures that are consistent with requirements in PCI DSS.
- Develop usage policies for critical technologies to define their proper use by all personnel. These include remote access, wireless, removable electronic media, laptops, tablets, handheld devices, email and Internet.
- Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.
- Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.

Review implemented security controls for effectiveness, and submit an attestation of PCI DSS compliance annually, to the Associate Vice President of Finance and Global Payments.

Disciplinary Actions

Violations of this policy may result in disciplinary action which may include termination for employees; a termination of employment relations in the case of contractors or consultants; or suspension or expulsion in the case of a student. Additionally, individuals are subject to loss of UTMB IR access privileges, civil and/or criminal prosecution.

References

- Texas Administrative Code Chapter 202
- Payment Card Industry, Data Security Standard
- UT System Policy, UTS-165