Baylor University

Policy Title: Payment Card Industry (PCI) Policy	**Policy Number:**
Date Issued: December 15, 2014	**Responsible Executive: Vice President of Finance**
Date Last Revised: March 30, 2022	**Responsible Office: Financial Services**

Payment Card Industry (PCI) Policy

Policy Statement

The purpose of this policy is to help assure that Baylor University (Baylor) is (1) being a good steward of personal information entrusted to it by its constituents, (2) protecting the privacy of its constituents, (3) complying with the Payment Card Industry Data Security Standard (PCI DSS), and (4) striving to avoid a security breach from unauthorized and inappropriate use of cardholders' information.

Reason for the Policy

Because of the substantial penalties and fines that can be levied against Baylor, Payment Card Industry (PCI) compliance is of the utmost importance.

Individuals/Entities Affected by this Policy

All employees who handle credit card data.

Exclusions

NONE

Related Documents and Forms

University Policies and Documents

Technology Usage Policy
Employee Personal Information
Handling of Confidential Information
Student Policy & Procedures
Network Usage Policies
Password Policies
Server Security Policy

1. PCI Policy

ITS Disaster Recovery Policy
Information Use Policy
PCI Security Standards Council
eCommerce Guidelines

Additional Information

Additional procedural and other information is available at Baylor's PCI website.

Definitions

These definitions apply to terms as they are used in this policy.

Critical Vulnerabilities	Vulnerabilities having a Common Vulnerability Scoring System v 2.0 score of 7 – 10, those causing a failing PCI scan, or those deemed by the CISO as critical
Remote Access	Connection from off the Baylor campus network to Baylor owned PCI equipment

Contacts

Subject	Contact	Telephone	Office email/web site
Policy Questions	Assistant Vice President for Financial Services and Treasury	254-710-8775	Dave_Clendennen@baylor.edu
PCI Compliance Questions	Payment Card Oversight (PCO) Committee		PCI-Information@baylor.edu PCI website
ITS	HelpDesk	254-710-4357	helpdesk@baylor.edu

Responsibilities

Departments	A. Contact the Financial Services Office prior to initially accepting tender for any product/service. B. Ensure all employees who have access to cardholder data are trained annually. C. Ensure only trained employees and employees with a need to know are allowed access to cardholder data. D. Use only Baylor approved equipment as detailed at the PCI website to process card information. E. Report suspected or confirmed cardholder data loss. F. Conduct refunds in accordance with Baylor policy.
PCO Committee	A. Review payment card processing to help ensure Baylor compliance with PCI DSS. B. Approve PCI policies and standards and review at least annually. C. Approve each merchant bank or processing contact of any third-party vendor that is engaged in, or proposed to engage in, the processing or storage of transaction data on behalf of Baylor – regardless of the manner or duration of such activities.

	D. Notify card companies of a breach in accordance current card companies' requirements. E. Approve new and/or modified PCI equipment/system requests.
Financial Services' Office	A. Conduct initial and recurring PCI training for all Baylor employees handling cardholder information. B. Track training records for all Baylor employees accessing customer card information. C. Track and provide credit card equipment to departments. D. Ensure that all employees accessing card information have had a background check.
Information Technology Services (ITS)	A. Review and recommend approval/disapproval of all new or modified systems/applications with PCI related functions to the PCO Committee per the Change Management policy contained herein. B. Perform investigations of all suspected or confirmed data loss. Notify the PCO Committee of suspected breaches. C. Ensure that all third-party vendors that accept credit cards include Baylor's PCI contract addendum prior to contract implementation and that they maintain PCI compliance. D. Approve/disapprove requests for remote access.

Principles

The PCI DSS was developed by MasterCard, Visa, Discover, American Express, and JCB to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS provides a baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process, or transmit cardholder data (CHD) and/or sensitive authentication data (SAD). Below is a high-level overview of the 12 PCI DSS requirements.

PCI Data Security Standards	
Build and maintain a secure network and system	**1.** Install and maintain a firewall configuration to protect cardholder data **2.** Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	**3.** Protect stored cardholder data **4.** Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	**5.** Protect all systems against malware and regularly update anti-virus software or programs **6.** Develop and maintain secure systems and applications

Implement strong access control measures	**7.** Restrict access to cardholder data by business need to know **8.** Identify and authenticate access to system components **9.** Restrict physical access to cardholder data
Regularly monitor and test networks	**10.** Track and monitor all access to network resources and cardholder data **11.** Regularly test security systems and processes
Maintain an Information Security policy	**12.** Maintain a policy that addresses information security for all personnel

Executive Summary

The following statements summarize Baylor‘s payment card policy:

- All payment card processing is subject to review by the PCO Committee to help ensure Baylor’s compliance with PCI DSS.
- The PCO Committee will review and provide approval/disapproval on PCI systems, applications, and equipment.
- Compliance with the PCI DSS is required of all Baylor employees and departments that accept, process, transmit, or store payment cardholder information.
- Sensitive authentication data (e.g., CVC2, CVV2, CID, PIN) must **never** be stored in any form.
- Only Baylor employees who are properly trained may accept and/or access cardholder information, devices, or systems which store or access cardholder information.
- Only PCI DSS compliant equipment, systems, and methods may be utilized to process, transmit, and/or store cardholder information.
- Each Baylor employee who has access to cardholder information is responsible for protecting that information in accordance with PCI DSS and Baylor policy and procedures.
- The events and circumstances of a suspected security breach which could negatively affect cardholder information or Baylor‘s compliance with PCI DSS must be immediately reported and investigated in accordance with the ITS Incident Response Policy.
- Background checks must be performed on employees who will be handling cardholder information prior to their access to credit card information.
- Vendors and service providers operating on the Baylor campus that accept or handle credit cards must execute a contract addendum assuring their compliance with PCI DSS. Non-Baylor employees who are acting on Baylor's behalf must comply with PCI DSS.

Data/Record Retention

1. Electronic storage of credit card data is prohibited. For any cardholder information to be stored, it must be documented by the department and approved by a designee of the PCO Committee.
2. Paper documents containing cardholder information must be treated as confidential and secured properly at all times. When not in use, documents containing cardholder information must be stored in a locked location.
3. Any paper documents containing credit card information must be limited to only information required for a business transaction, accessed only by individuals who have a business need, stored in a secure location, and destroyed via approved methods once business needs no longer require retention.
4. Storage of documents containing credit card information must not exceed 45 days and should be limited whenever possible to only 3 business days. Secured destruction must be via cross-cut shredding, either in house or with a third-party provider with certificate of disposal. Delete any electronic cardholder information from databases, including computer hard drives, CDs, disks, and other external storage media, using PGP shredder or other mechanism approved by Baylor ITS.
5. Inventories of paper documents containing cardholder information must be conducted by the owning department at least quarterly to ensure secure destruction of stored data that exceeds defined retention policy.
6. Neither the full contents of any track for the magnetic strip nor the card validation code may be stored in a database, log file, paper files, or point of sale product once authorization has been approved.
7. All cardholder data is stored and backed up by Baylor's payment vendors. Recovery of information will be coordinated between Baylor and its vendors.

Usage

1. Cardholder information may not be sent or accepted via unencrypted electronic communication (e.g., email, instant messaging, chat, text messaging).
2. Use of PCI technologies must be in accordance with current Network Usage Policies and Information Use Policy.
3. Credit card information must be processed utilizing Baylor provided P2PE certified payment terminals. At no time, shall a Baylor employee use a keyboard or other non-certified payment terminal to input a credit card into Baylor systems for processing.
4. Access to cardholder information must be limited to those individuals whose job requires access.
5. An authorization approval code, a 6-digit code that shows the transaction was approved, must be obtained for all transactions processed.
6. Users found in violation of any aspect of Baylor's PCI policy will immediately have their PCI system access disabled pending further investigation.

Remote Access

Only authorized personnel are allowed to remotely access any Baylor owned PCI asset. All remote access requires two-factor authentication in order to access the equipment. Administrative or remote access will not be allowed until the user has the approved two factor system. Requests for remote access must be submitted to the CISO by e-mail to pci@baylor.edu.

User Account Control

1. Users must have a unique user ID for access to any PCI equipment or payment application.
2. Passwords must have a minimum of three (3) of the following: upper case letter, lower case letter, number, and/or special character.
3. Passwords must be a minimum of seven (7) characters long.
4. In accordance with PCI requirement 8.5.4, ITS will terminate any user account immediately upon notification an employee has terminated employment with Baylor.
5. Application passwords must be changed every ninety (90) days.
6. Group, shared, or generic IDs and passwords are not to be used on any PCI application or system.
7. Users must lock their screens if leaving their computer unattended for more than fifteen (15) minutes.

Note: BearID password standards meet the standards outlined above.

Training

1. Employees who handle cardholder information must receive training and acknowledge their understanding of their responsibility for compliance with Baylor policies and procedures prior to being granted access to PCI systems or data.
2. Employees who handle credit card data are required to maintain annual training on PCI DSS and the importance of compliance and must acknowledge that they have read and understand Baylor's PCI policies and procedures.

Note: Contact the Financial Service's Office to schedule training.

Risk Assessment

In accordance with PCI requirements, Baylor conducts an annual assessment of the PCO approved technology for credit card processing, procedures, and policies. Baylor's Internal Audit department is responsible for conducting all assessments and providing recommendations to ITS on changes or enhancements to increase Baylor's PCI compliance posture.

Baylor ITS Security is responsible for requesting the assessment prior to the previous review's expiration.

Change Management

Change management consists of two separate functions, infrastructure modification and patch management. Infrastructure modification includes, but is not limited to, the installation of new applications/hardware, version/revision upgrades for software, and security policy changes to network systems/software. Patch management is the application of vendor supplied security and operational patches to server and network operating systems or firmware.

Infrastructure Modification

A formal request for modification will be required under the following circumstances:

- Modification to the network infrastructure, security controls, hardware, operating systems (vendor patch management process below), applications, database, files, fields, etc.
  - Modification includes version and revision upgrades to software, firmware, and operating system or application and policy changes to network or server infrastructure.
  - Existing electronic processes internal to ITS for policy changes meet this requirement.
- Addition of new elements – hardware or software – that use or extend delivered system functions including data.
- On approval, modifications will be completed during Baylor's scheduled maintenance window.

The request must be submitted electronically to the department chair/director for their approval. The department chair/director will submit approval to ITS, pci@baylor.edu, and provide the impact of the change, a test plan to verify the change, roll back plan, and requested timeline for delivery.

Patch Management

Critical patches will be applied within thirty (30) days of notification of a patch release. All other patches will be implemented within ninety (90) days of notification. Patches should be tested prior to installation to ensure no impact to operations. If testing is not practical, patches should be installed in a staggered implementation to mitigate potential impacts to PCI operations.

Prior to installation, the patches being installed must be submitted to the CISO, along with potential impact and a roll back plan. The CISO may determine that a critical patch must be implemented sooner than thirty (30) days.