Policy Title: Payment Card Industry (PCI) Policy	**Policy Number:**
Date Issued: December 15, 2014	**Responsible Executive: Vice President of Finance**
Date Last Revised:	**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 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, 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
Directory Information Policy
Employee Personal Information
Handling of Confidential Information
Student Policy & Procedures
Network Usage Policies
Password Policies
Server Security Policy
ITS Disaster Recovery Policy
Information Use Policy

PCI Security Standards Council
eCommerce Guidelines

Additional Information

Additional 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 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 (Appendix C) 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 with Appendix B. 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. Maintain all PCI server and network infrastructure. D. Provide user account access and control for PCI networks and applications. E. 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. F. Approve/disapprove requests for remote access.

Principles

The Payment Card Industry Data Security Standard (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 Payment Card Oversight (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 log data from systems in scope of Baylor's PCI network, to include but not limited to servers, network switches, intrusion detection/prevention systems, and clients, will be stored centrally on the PCI network with search access provided to the main campus network. Logs will be maintained for one year unless otherwise required for retention by the Chief Information Security Officer (CISO). The entire year of logs will be maintained as immediately searchable.
8. All cardholder data is stored and backed up by Baylor's payment vendors. Recovery of information will be coordinated between Baylor and its vendors.
9. PCI network configuration data will be backed up locally.

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 PCI network, 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 managements 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.

Appendix A – PCI Standard Operating Procedures

Daily

- Review logs of Baylor owned PCI equipment via Splunk
- Follow-up anomalous results with Vulnerability Management and CISO
- Verify AV connectivity for all servers, check the AV server to ensure latest signatures are downloaded

Weekly

- Update Linux server virus definitions
- Review virus scan logs on all servers
- Review the weekly Qualys external scan for vulnerabilities

Monthly

- Run/review the monthly external PCI scan from Qualys PCI scanner
- Work with Vulnerability management to correct any failing scan results
- Review user accounts for inactivity
- Review servers with system administrators to ensure that AV has not corrupted any system files

Quarterly

- Review annual/new training to ensure no users are missing training
- Deep dive into logs for all systems and rule sets on File Integrity monitor to create new rules if necessary
- Verify Thin Client software is current and protected
- Disable/Delete accounts with 90 days or more of inactivity
- Review GPO policy on servers and update if needed

Semi-Annually

- Review and update rules on all PCI firewalls
- Schedule annual risk assessment with Internal Audit
- Work with CISO to schedule an external scan of PCI network
- Review 2X accounts with departments to get rid of users no longer accessing the network

Annually

- Review all policies that apply to PCI and make changes as necessary
- Review the annual risk assessment report
- Request PCI compliance documentation from vendors

Appendix B – Credit Card Brand Breach Response Procedures

Bank of America – Responding to a Breach
See '*Responding to a Breach: A guide provided by Bank of America Merchant Services*' at http://merch.bankofamerica.com/documents/10162/12961/respondingbreach.pdf.

MasterCard – Responding to a Breach
Follow the steps set forth in the *http://www.mastercard.com/us/merchant/pdf/Account_Data_Compromise_User_Guide.pdf.*

Visa – Responding to a Breach
Follow the steps set forth in the resource:
http://usa.visa.com/download/merchants/cisp_what_to_do_if_compromised.pdf.

American Express – Responding to a Breach
See Section 2 of:
https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=merchinfo&ln=en&frm=US&tabbed=breach.

Appendix C – Approved Equipment

BlueFin ID Tech SREDKey

BlueFin PAX A80

BlueFin PAX A920

BlueFin PAX A920 Pro

Other equipment must be approved my PCO Committee and meet PCI-PTS certification requirements.

Appendix D – Baylor Specific Card Procedures

Card Present

Sales

1. The payment card features, valid date(s), and signature (if required) must be examined. (*See Card Examination section below.*)
2. The person presenting the card must be the cardholder.
3. If a signature is required, the cardholder must sign the merchant copy of the transaction receipt.
4. A transaction receipt must be provided to the cardholder at the time the transaction is completed.
5. The transaction receipt must not include the full 16-digit account number; only the last four digits may be displayed.
6. The merchant copy of the receipt must be retained in accordance with University's record retention policies.
7. Cash in excess of the sales amount must not be given to the cardholder.

Refunds

1. A refund must be processed using the same card used by the cardholder to make the original purchase.
2. The cardholder must sign the merchant copy of the refund receipt.
3. A refund receipt must be provided to the cardholder at the time the refund is completed.
4. The merchant copy of the refund receipt must be retained in accordance with University's record retention policies.

Card Examination

The following should be examined before accepting a payment card transaction:

a. Card features
    i. General
        1. The card logo should be printed on the card
        2. The 1st card number should match the type of card
        3. The CVC2/CVV2/CID should be identified
        4. The card and signature panel should not show signs of tampering
    ii. Brand-specific

MasterCard	Visa

a. MasterCard logo	a. Visa logo
b. Card number starts with a "5"	b. Card number starts with a "4"
c. 3-digit CVC2 on back	c. 3-digit CVV2 on back
American Express	Discover
a. American Express logo	a. Discover logo
b. Card number starts with a "3"	b. Card number starts with a "6"
c. 4-digit CID on front	c. 3-digit CID on back

b. Valid dates
    i. The transaction date must fall within the valid dates indicated on the card.
c. Signature
    i. The signature on the card must compare favorably to the signature on the receipt.
    ii. If no signature is present on the back of the card, a positive ID must be reviewed.
    iii. If there are two signatures on the back of the card, the card must not be accepted.

Card Not Present

On-Line Transactions

1. All on-line payment card processing must be coordinated through Information Technology Services (ITS) and use a solution approved by the Payment Card Oversight (PCO) Committee.
2. Web forms used to collect information for internet sales must include the following:
    a. Description of the goods/services offered
    b. Description of cancellation/return policy
    c. Customer service contract
    d. Links to Baylor's Web Site Privacy Statement and PCI policy
3. Payment card information must not be entered on behalf of a customer into an on-line form unless a terminal approved by the PCO Committee is used. Such devices must be used only for approved applications (those relating to the acceptance of payment cards).

Refunds

A refund must be processed using the same card used by the cardholder to make the original purchase.

Mail Order Transactions

1. Mail order forms must clearly identify the following:
    a. Merchant name
    b. Merchant address
    c. Description of goods/services offered
    d. Transaction amount
2. Mail order forms must collect at least the following information:
    a. Cardholder name
    b. Billing address
    c. Shipping address (if different)
    d. Card type (MC/VI/AMEX/DISC) – in a detachable section at the bottom of the form
    e. Account number – in a detachable section at the bottom of the form
    f. Expiration date – in a detachable section at the bottom of the form
3. Mail order forms **must not** request the cardholder's 3 or 4-digit card verification code (CVC2, CVV2, CID).
4. Items 2. d.-f. should be requested. This section must be in a detachable section at the bottom of the form, removed and destroyed using a cross-cut shredder as soon as possible after the transaction is complete and the cardholder information is no longer needed.
5. The Authorization Approval Code must be recorded and retained on the mail order form.

Transactions Processed by Student Account's Office

1. Documents containing cardholder information must be securely stored in a locked location when not in use. Any documents containing cardholder data must be destroyed as soon as possible after the transaction is complete and the cardholder information is no longer needed.
2. Cardholder data must be handwritten – never recorded or stored electronically – and securely delivered in person to the Student Account's Office as quickly as possible for processing.

Appendix E – PCI Incident Response Procedures

General Response Procedures

1. The user will report the incident to a member of the ITS security team in accordance with the Baylor Incident Response policy. Do not include any credit card information in the report.

2. ITS security will investigate the incident and report to the Chief Information Security Officer (CISO).
    A. Ensure compromised system is isolated on/from the network.
    B. The ITS investigator will gather, review, and analyze all centrally maintained system, firewall, file integrity, and intrusion detection/protection system logs.
    C. The ITS investigator will scan the locally maintained system and other logs, as needed for potential PCI data.

3. The investigator officer will report the number, type, and location of all data found to the CISO. Based on the investigation, the CISO will determine if the data was breached. The CISO will:
    A. appoint or contract the appropriate people to conduct appropriate forensic analysis of compromised system.
    B. contact Internal Audit, PCI Oversight Committee, University Police, and/or other law enforcement agencies as appropriate.
    C. make forensic and log analysis available to appropriate law enforcement or card industry security personnel.
    D. assist law enforcement and card industry security personnel in investigative process.

4. ITS Security will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, credit card processors, etc.) as necessary.

5. The CISO will determine if policies and processes need to be updated to avoid a similar incident in the future.

E-mail Incident Response Procedures

In the event that a Baylor employee or person acting on Baylor's behalf receives cardholder information, e.g. credit card number, via e-mail, you should:

1. Make a note of who sent the e-mail (forwarded from within the University or sent directly from the customer).

2. Notify the Baylor ITS security team (710-2711/709-5699) with the circumstances of the e-mail and include the following:
    - Date and Time
    - From Address
    - To Address
    - Subject Line (as long as it doesn't contain credit card information)
    - Confirmation that you will permanently delete the e-mail
3. Do **NOT** process the credit card received via e-mail.
    - Reply to the sender (making sure to delete cardholder information) with the following text: "Baylor University cannot accept e-mailed credit card information in accordance with PCI compliance requirements and for the protection of our valued customers. In order to securely process your credit card, we will be calling to obtain the information by phone."
    - Contact the customer or donor directly via phone/in person, reinforce that we cannot accept credit cards via e-mail, and request that they provide the credit card number over the phone.
4. Permanently delete the e-mail (contact the ITS HELP desk, 254-710-4357, if you have questions regarding this procedure) as follows:
    - Shift+Delete, with confirmation
    - Select the Folder tab
    - Click "Recover Deleted Items"
    - Find the e-mail message and delete it from that list by clicking "X"
5. If the e-mail was forwarded from within the University, notify the individual that we cannot accept credit cards via e-mail. If the individual has questions, he/she can contact the PCO Committee (pci@baylor.edu).
6. ITS will install and run a program to scan any involved computer(s) to ensure the card information is completely deleted.