Credit Card Transaction Policy

Effective Date: 04/30/2010
Last Revised: 07/10/2015
Last Reviewed: 02/21/2016

Audience

All Staff

Policy

All transactions (including those which are electronically based) used to receive payment to MBI that involve the transfer of credit card information must be performed on systems approved by the Moody Bible Institute Information Technology Services Department. All specialized servers approved for this activity must be housed within Information Technology Services and administered in accordance with the requirements of all Moody Bible Institute policies and the PCI Data Security Standard (PCI DSS). Moody Bible Institute is involved in PCI DSS compliance and is subject to examination of system security and configuration to ensure cardholder information is securely maintained. The Controller's Office & Information Technology Services will be responsible for verifying compliance with industry best practices for conducting electronic payment transactions through Data Capture / Point of Sale machines (Credit Card Terminals). All media used for credit cards must be destroyed when retired from use. All hardcopy must be shredded prior to disposal.

Definitions

A. The PCI Data Security Standard is designed to ensure that all merchants that store, process, or transmit cardholder data, protect it properly. To achieve compliance, merchants and service providers must adhere to the Payment Card Industry (PCI) Data Security Standard.
B. *PCI:* The PCI Standard is the result of collaboration between the four major credit card brands to develop a single approach to safeguarding sensitive data. The PCI standard defines a series of best practices for handling, transmitting and storing sensitive data. A list of all POS devices will be logged along with procedures identifying maintenance and training.
C. *Cardholder Data:* Cardholder data is any personally identifiable data associated with a cardholder. This could be an account number, expiration date, name, address, EFT's, banking or routing number or any card verification data.

Procedures

A. No electronic credit card numbers should be transmitted or stored in any other system, personal computer, or e-mail account.
B. Physical cardholder data must be locked in a secure area, and limited to only those individuals that require access to that data. In addition, restrict access to data on a "need to know" basis.
C. Store only essential information. Do not store any card verification data. Do not store the full contents of any track from the magnetic stripe (on the back of the card, in a chip, etc.)
D. Credit card information should be retained for the minimum amount of time necessary. Storage amount and retention time is limited to that which is required for business, legal, and/or regulatory purposes, as documented in the Credit Card Data Retention & Disposal Policy. All media used for credit cards must be destroyed when retired from use. All hardcopy must be shredded prior to disposal.
E. All departments must comply with the PCI Data Security Standards.
F. Exceptions to this policy may be granted only after a written request has been submitted and approved by the Vice President of Information Technology Services.

Documents

PCI DSS 3.1,7.1, 9.9, 9.10 & Credit Card Data Retention & Disposal Policy

Contacts

If you have questions or concerns about the execution of this policy, you may contact the Information Technology Services Support Center 312.329.4067 or ITS@moody.edu for assistance.