ACU Payment Card Security Policy

Responsible Departments: Finance and Information Technology
Responsible Administrators: Chief Financial Officer; Chief Information and Planning Officer
Effective Date: June 1, 2011
Reviewed/Updated Date: April 9, 2018
Date of Scheduled Review: Each anniversary date of the effective date

Purpose: The purpose of this security policy is to help assure that Abilene Christian University is (1) being good stewards 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 Standards, and (4) striving to avoid a security breach from unauthorized and inappropriate use of cardholders' information. This policy works in conjunction with ACU's Policy on Identity Theft Red Flag Rules in accordance with the Federal Trade Commission (FTC) and Fair and Accurate Credit Transaction Act (FACTA).

Scope: This security policy is intended for:

- Any individual who accepts, captures, stores, transmits, or processes credit or debit card payments received for the purchase of University products and services, for contributions, etc.
- Any individual who supports University efforts in accepting, capturing, storing, transmitting, and/or processing credit or debit card information such as technical support staff members whose roles involve access to computer hardware and software involved in accepting, capturing, storing, transmitting, or processing credit or debit card information, and any individuals tasked with destroying credit and debit card information, etc.

Definitions:
Cardholder Data: Cardholder data refers to all information from a credit card or debit card that is used in a transaction. Commonly used elements of cardholder data include the primary account number (PAN), cardholder name and expiration date displayed on the front of the card.

Sensitive Authentication Data: Sensitive authentication data is security related information used to authenticate cardholders and authorize card transactions. Sensitive authentication data elements include magnetic stripe data, personal identification number (PIN) or the encrypted PIN block, and the card validation code - the three or four digit number security code found either on the front or on the back of a card (a.k.a. CVV, CVV2).

Policy:
The following statements comprise Abilene Christian University's payment card security policy:

1. Compliance with Payment Card Industry Data Security Standards (PCI-DSS) as published by the PCI Security Standards Council is required of all ACU employees and departments that accept, process, transmit, or store payment cardholder information.

2. Only authorized ACU employees who are properly trained for PCI-DSS compliance may accept, capture, store, transmit, or processes cardholder data or access cardholder information, devices, or systems that store or access cardholder information:
    - ○ Employees new to the role of handling cardholder data must be trained prior to receiving credit/debit card handling duties.
    - ○ Employees whose payment card handling duties preceded implementation of this policy should receive training as soon as possible.
    - ○ The content of the training program must be reviewed and approved by the Controller in Financial Operations.
    - ○ Evidence of successful completion of the training program for each applicable employee is required on an annual basis and will be documented by the employee's signature on a certification of training form or completion of an approved online training delivery method.
3. Only PCI-DSS compliant equipment, systems, and methods that are approved by the Financial Operations Team may be utilized to process, transmit, and/or store cardholder information.
4. Critical or high-risk technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants [PDAs], and internet usage) may be used to handle or transmit cardholder data only if approval is obtained from Financial Operations that defines the following:
    - o Authentication for use of the technology;
    - o A list of all such devices and personnel with access;
    - o A description of the acceptable uses of the technologies;
    - o When applicable, automatic disconnect of remote-access technologies after a specific period of inactivity.
    - o Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.
    - o Cardholder data may not be entered, processed, or transmitted by an ACU employee or contractor on a computer connected to the internet unless the computer is placed within a separate and secure LAN and only if internet access on the applicable computers is restricted to only the websites necessary to complete transactions.
5. Third-party vendors processing or accessing cardholder data must be PCI-DSS compliant and must, prior to their engagement, provide Financial Operations with a copy of the Vendor’s Attestation or Certificate of Compliance with PCI DSS for their applicable validation types. If cardholder data is shared with service providers, the following items apply:
    - o A list of such service providers must be maintained;
    - o A written agreement must be obtained from such service providers indicating the service providers are responsible for the security of cardholder data the service provider possesses.
    - o Financial Operations will monitor the status of service provider compliance with PCI-DSS at least on an annual basis.
6. Each ACU employee or contractor acting on behalf of ACU who has access to cardholder information is responsible for protecting that information in accordance with PCI-DSS and University policy and procedures.
    - o All media (consisting of all paper and electronic data containing cardholder data) must be physically secured at all times, and the transport of any such media containing cardholder data, if applicable, must be approved by management and tracked by a log or other method.

7. Cardholder data must be destroyed or deleted so that it is not recoverable as soon as it is no longer necessary for processing transactions.
    - Paper documents containing cardholder data must be destroyed by using a cross-cut shredder.
8. Under no circumstances may unprotected primary account numbers be received or transmitted via end-user messaging technologies (for example, email, text messaging, chat, etc.).
9. Sensitive authentication data may never be stored under any circumstances, even if encrypted, subsequent to the authorization of a transaction. If sensitive authentication data is received and deleted or destroyed, each merchant must have processes in place to ensure that the deleted or destroyed data is unrecoverable.
10. To comply with PCI-DSS requirements, merchants transmitting cardholder data via the internet must complete quarterly internal and external vulnerability scans (external scans must be performed by an approved scanning vendor) and vulnerabilities identified during scans must be corrected in a timely manner.
11. Financial Operations will maintain and communicate an Incident Response Plan to provide specific guidance on how to respond in the event of a suspected security breach, which could negatively affect cardholder information or the University's compliance with PCI-DSS. Any such event must be immediately reported to the Controller in Financial Operations and the Director of Technology Support Services for an appropriate response in accordance with the Incident Response Plan.
12. Non-ACU employees who are acting on ACU's behalf must comply with PCI-DSS. Vendors/Merchants and service providers operating on the ACU campus that accept credit cards must execute a contract addendum assuring their compliance with PCI-DSS.
13. Each merchant that accepts credit card payments must complete an annual Self Assessment Questionnaire (published on the PCI Security Standards Council website) to be reviewed by the responsible administrator or designee.

Failure to comply with these principles, as implemented in this Payment Card Security Policy, may result in the revocation of the ability to process credit and debit card transactions and/or could lead to disciplinary action. Because of the substantial penalties and fines that can be levied against Abilene Christian University, PCI-DSS compliance is of the utmost importance for all transactions involving payment cards.