TRINITY INTERNATIONAL UNIVERSITY

TIU POLICY:	**Credit and Debit Card Payments Security Policy**
TIU POLICY #:	**P-107**
STATUS:	**Approved, January 2015** **Updated, May 2015**

I. PURPOSE:

To specify policy for compliance with Payment Card Industry (PCI) Data Security Standards for handling credit and debit card transactions.

II. SCOPE:

Trinity International University (University) seeks to be good stewards of sensitive information provided by others through credit and debit card payments. Because the role of the University is to ensure the protection of payment card information and satisfy PCI requirements, this policy applies to any individual or department involved in the acceptance, capture, storage, transmission and/or processing of card payments received by the University.

III. POLICY:

A. Background

To reduce their losses due to credit card fraud, five members of the payment card industry, Visa, Master Card, American Express, Discover and JCB, banded together to develop security standards for any organization that accepts, captures, stores, transmits and/or processes credit card information either manually or through an automated system. This set of standards is referred to as the Payment Card Industry's Data Security Standard, or "PCI-DSS."

PCI-DSS is enforced through the contracts that the University, as a merchant account holder, has with its merchant bank. Penalties for non-compliance can include increased credit card transaction fees, a suspension of credit card privileges, and fines in cases where an account is compromised.

For additional information about PCI-DSS, please visit the Payment Card Industry's Web site at: https://www.pcisecuritystandards.org.

B. PCI-DSS Compliance Requirements

The following requirements are necessary for the University compliance.

1. Authorized individuals: The following requirements must be satisfied before an individual is authorized to accept, access or support systems that store credit or debit card information:
   a. The individual should be a full-time employee of the University. A high level of discretion should be given prior to utilizing any part-time employees in roles that involve the handling of sensitive credit card information. In instances where it is deemed appropriate by a supervisor, adequate training should be conducted by the supervisor and a background check should be performed prior to performing duties involving sensitive information. The individual must be authorized and trained by their supervisor prior to taking on their credit or debit card handling duties.
   b. The individual must acknowledge his or her understanding of this policy and must confirm his or her commitment to comply by signing the "Credit and Debit Card Security Agreement" (Form 107-A).
   c. Departments handling credit or debit card transactions must segregate, to the extent possible, all duties related to data processing and storage of credit and/or debit card information. A system of checks and balances should be put in place in which tasks are performed by different individuals in order to assure adequate controls. For example, the same person should not process credit or debit card transactions/refunds and perform the monthly credit and debit card reconciliation.

2. Acceptable payment methods: Credit and debit card payments may be accepted only using the following methods:
   a. in person
   b. via telephone
   c. via fax
   d. via physical mail (email and instant messaging are strictly forbidden)
   e. through a PCI-DSS-compliant automated system that is entirely hosted by a PCI-DSS-compliant third party organization and approved by Information Technology
   f. through an automated system that is hosted in the University data center that does not accept, capture, store, transmit or process credit or debit card information itself, but refers the customer to a PCI-DSS-compliant system hosted by a third party organization and approved by Information Technology

3. Protection of payment card information: Each person who has access to credit or debit card information is responsible for properly safeguarding and protecting the integrity and privacy of the following information:
   a. Credit or debit card number

b. Credit or debit card expiration date
c. Cardholder Verification Value (CVV2) – the 3- or 4-digit code number generally located on the back of the credit or debit card.
d. Personal identification number (PIN)
e. Cardholder's name, address and/or phone number when used in conjunction with the above fields
f. Point-of-sale devices must be configured to print only the last four characters of the credit or debit card number on both the customer and the merchant receipts, and on any reports that may be produced by the device
g. It is prohibited to store sensitive cardholder data in any University system and/or departmental server, third-party software, personal computer, cash register system, e-mail account, portable electronic device (including, but not limited to, laptop, flash drive, floppy disc, CD, PDA, and external or portable hard drive), or on paper.
h. Credit and debit card information must be destroyed as soon as it is no longer necessary.
i. Suspected theft of credit or debit card information must be reported immediately to Information Technology.

4. Documentation of procedures: Each department that handles credit and debit card information must have documented procedures for complying with item #'s 1-3 above.