

Effective Date: November 2020
Previous Version: None
Policy Owner: Chief Financial Officer
Approved by: President
Approval Date: 11/1/2020

PAYMENT CARD ACCEPTANCE AND DATA SECURITY

Policy Summary

Credit and debit cardholder data information is regulated information that must be appropriately secured. NewU is required to be compliant with the Payment Card Industry (PCI) Data Security Standards, and is committed to providing a secure environment to protect against both loss and fraud related to cardholder information. This compliance included securely processing, storing, transmitting and disposing of card and debit cardholder information.

Related Regulations

The purpose of this policy is to promote protection of cardholder data in accordance with the Payment Card Industry Data Security Standard (PCI-DSS). Failure to comply with the PCI-DSS standards may result in fines, loss of ability to process payment cards, and reputational damage to NewU.

Scope

The Policy on Payment Card Acceptance and Data Security applies to all NewU Staff, Faculty, Students and External entities that intend to use NewU Technology Services.

Policy

Cardholder data is designated as regulated data per the Information Security Policy. NewU offices and members of NewU community involved in processing payment card transactions are responsible for protecting such data, and for following the information security practices and policies set forth herein, including those referenced under the Related Information section below. The CFO is responsible for issuing all credit card merchant identification accounts, for arranging NewU-approved payment card acceptance services, and for approving payment card procedures. NewU offices may not collect, process, store, transmit or display payment card information without advance approval from the CFO. This requirement applies to all payment card transactions whether conducted in person, via telephone, fax, mail, internet, or through a NewU-approved third-party vendor on behalf of a NewU. NewU offices with a business need to process payment card transactions must contact the CFO or his/her designee in advance of accepting any payment to obtain a merchant identification account, training, and the appropriate NewU approved secure payment processing method(s). Any NewU office that manages or contracts with external users, including but not limited to tenants, caterers, business establishments, volunteer organizations, or event organizers that intend to use external payment card services, must

also contact the CFO to request a review and approval. Use of NewU wired or wireless networks for accepting payment cards is strictly prohibited.

Definitions

Cardholder Information: Any information pertaining to credit or debit card, including but not limited to: card number, cardholder name, card verification (CVC, CVV, or CID) number, expiration date, personal identification number (PIN), password, etc. Credit or debit cards include but are not limited to those issued by Visa, Mastercard, Discover, Diners Club, and American Express.

[End]