Primary Contact:
Dayma Blanco, PCI *Compliance Manager*
Treasury Operations
(305) 284-1667
d.blanco@miami.edu

IT Security: ciso@miami.edu

MIAMI

Merchant On boarding Checklist

The following must be completed in order to obtain a Merchant ID to start processing credit cards and to remain in compliance with Payment Card Industry Data Security Standards (PCI DSS):

- ☐ **Participate in Onboarding Merchant Call with UM PCI Team and UMIT Applications**
- ☐ **Complete Request For Service (RFS) Form**
- ☐ **Complete Merchant Card Processing Request Form**
- ☐ **Complete UM Merchant Request Form**
- ☐ **Complete Bank of America Cash Pro Request Form**
- ☐ **Complete Nelnet Set Up Form**
- ☐ **Complete Payment for Attributes Form**
- ☐ **Include 10 Elavon Web Requirements on Departmental website**
- ☐ **Create Procedures for Credit Card Processing**

PCI requires that all merchants must add procedural documents for collecting, recording, and reconciling sales and refunds to accompany policies to ensure that day-to-day business practices conform to policies. Include specific staff/or positions responsible for process steps ensuring duty segregation, and independent review and reconciliation of transaction data.

☐ **Review UM Credit Card Processing & Security Policy** (https://umiami.policystat.com/policy/5524331/latest/) UM requires that all staff, faculty, and/or students, who in their work are either asked to handle payment cards or supervise those that handle payments must read and comply with University Credit Card Processing & Security Policy.

☐ **Vendor/Service Provider/Hosts Documentation** If you are planning to use third party vendors, service providers, or hosts to process credit cards, PCI requires that you maintain a contact list, obtain a written agreement that includes an acknowledgment that the service providers are responsible for the security of cardholder data the service providers possess, and monitor their compliance at least annually.

☐ **Training** UM Merchants are required to complete PCI Awareness & Cybersecurity Awareness training annually. Both trainings can be found in ULEARN

☐ **PCI Best Practices**

- All credit cards come with a secure code (CVV, CVV2) which acts as a security control to prove the card is in hand. This value must NEVER be written down, even for a moment.
- All hardcopy documents containing credit card data must be kept in a secured location from the moment the document is received, until the transaction is processed.
- All credit card information should be put through a crosscut shredder after the transaction is processed, or in an approved sealed document disposal bin.
- If credit card information will be stored within a file cabinet accessed by multiple individuals, a paper log must be implemented to track each time someone accesses the file cabinet, regardless if they are accessing credit card information or not.
- The entire credit card number must never be kept without an approved business reason.