Allowable Processing Methods

I. OVERVIEW – WHY THE PROCESSING METHOD MATTERS

A Unit that accepts payment cards (credit or debit cards) is defined as a Merchant and must comply with the MSU Merchant Services Policy and all the applicable Payment Card Industry Data Security Standard (PCI DSS) requirements. All people, processes, systems, solutions, devices, and applications that are involved in processing payment cards are included in the scope of what needs to be compliant. Compliance is easier and less costly to achieve and maintain when the processing method chosen is one which meets the business needs with the minimal scope. This approach will also reduce the University’s overall risk and effort to maintain compliance. Furthermore, compliance is evaluated at the University level such that noncompliance by one University location causes the entire University to be noncompliant.

II. ALLOWABLE METHODS OF ACCEPTING PAYMENT CARDS

A. Wired network or phone lines are allowed. Wi-Fi is not allowed.

B. Centrally Supported Application – CASHNet
   1. Storefront – Customer transaction and payment page are both hosted on the CASHNet server.
   2. Checkout – Customer transaction is handed off to CASHNet at the point of payment.
   3. Changing the type of store – Changing from either a Checkout to a Storefront type of store (or vice versa) can result in a change in PCI reporting requirements and therefore needs Cashier’s Office pre-approval.

      Note: Effective January 1, 2015 with PCI DSS version 3.0, CASHNet Checkout stores will be subject to more stringent requirements. Units should try to convert to CASHNet storefronts or begin securing their web apps and environment per PCI DSS version 3.0 immediately.

C. Card Swipe Terminal (Land line)
   1. Stand-alone dial-out swipe device attached to an analog phone line. This is the preferred method when card is present.
   2. Also appropriate for Merchants that process orders received via US mail, over the phone, or by fax. Note that the fax machine must connect via a dedicated phone line; it cannot be on a network that is connected to the Internet.

D. Mobile Card Swipe Terminal (Cell phone plan, GSM connectivity)
   1. A specific model, approved by the Controller’s Office, stand-alone swipe device that connects via a cell phone plan and has wireless (Wi-Fi) capabilities disabled.
   2. Note, this is not a cell phone, but a device that uses a cell phone technology.

E. Ethernet Card Swipe Terminal (IP-Ethernet)
   1. Must have a properly configured hardware firewall.
   2. Contact the Cashier’s Office for acceptable models.
F. Card Swipe Terminal (Loaner)

2. Available on first-come, first-serve basis for a small monthly fee.

III. Methods Not Allowed

A. Wireless (Wi-Fi)

B. Smart phones, tablets, or any similar digital device.

C. Any solution in which payment card data is entered by an MSU representative (employee, volunteer, etc.) on behalf of a customer/donor into an MSU-owned device connected to the Internet.

D. MSU-owned device connected to the Internet that is offered to customers for the purpose of entering their own payment card data (e.g., kiosk).

E. Any application/solution/service/device that is not specifically validated as being PCI compliant.

F. Any other application/solution/service/device that has not been approved for general campus use by the MSU Controller’s Office or that is not listed in this document under Allowable Methods.

References

Cashier’s Office – Accepting Credit Cards page
http://ctlr.msu.edu/CreditCard/Default.aspx

CASHNet at MSU
https://paymentsupport.ais.msu.edu/cashnetatmsu.asp

Manual of Business Procedures, Section 17
http://ctlr.msu.edu/combp/mbp17EBS.aspx