Payment Card Processing Policy

Objective

The purpose of this policy is to establish procedures for processing Payment Card and/or Cardholder Data provided to Suffolk University and ensuring that such information is protected in accordance with University Policies and Payment Card Industry Data Security Standards (PCI-DSS) requirements for transferring, handling and storage of Payment Card and/or Cardholder Data.

Applicability

This policy applies to all University departments, individuals and organizations involved in the storing, processing, transmitting, or receiving of Payment Card and/or Cardholder Data at Suffolk University.

Definitions

Acquiring Bank: An acquiring bank is a financial institution that provides merchants with credit card processing or merchant accounts. The acquiring bank works directly with the merchant and acts as a processor to authorize card purchases and provide settlement.

Background Check: The review of a person's prior history with regards to financial fraud risk. Examples of background checks include previous employment history, criminal record, credit history and reference checks.

Cardholder Data: Cardholder data is personally identifiable data associated with a cardholder's account, including account number, expiration date, name, address, social security number, card validation code or card identification number.

University Merchant: A University Merchant is a Suffolk University department or organizational unit that accepts Payment Cards for products, services or donations.

Payment Card: A payment card can be a credit card (Visa, AMEX, MasterCard, Discover, etc.) or a debit card.

University Information Resource: A University Information Resource is any tool, device, piece of equipment, or system used to create, collect, record, process, store, retrieve, display or transmit University Information, including but not limited to e-mail, mainframes, servers, computers, laptops, personal digital assistants (PDA), telecommunication resources, fax machines, printers, file cabinets, software and embedded technology.

Policy

University Merchants are required to follow the rules and procedures outlined below to protect customers' Payment Card and Cardholder Data.

Suffolk University limits Payment Card and Cardholder Data processing to the following methods:

- In-person swipe transactions
- Customer initiated Web-based entry
- Direct input into credit card device via phone-in order

The following Payment Card/ Cardholder data processing methods are prohibited:

- Payments via fax machine.
- Paper processing (including e-mail) of Payment Card/Cardholder Data information.

Storage of electronic credit card data on Suffolk University computers, servers, laptops or storage media such as CDs or flash drives is prohibited.

Payment Card / Cardholder data may not be sent through campus mail nor be transported by hand from one unit or department to another unit or department.

Background checks are required for any employee or student involved in or directly interacting with Payment Card/ Cardholder Data processing. The background check must be completed through Human Resources prior to the employee or student involved in or directly interacting with Payment Card/ Cardholder Data.

PCI-DSS Training

To ensure appropriate handling of Payment Card and Cardholder data, all University Merchants that interact with Payment Card and Cardholder Data must attend PCI-DSS training scheduled through Human Resources when initially accepting the responsibility and annually thereafter.
If a University Merchant does not attend this workshop, the University Merchant's authorization to handle Payment Card and Cardholder Data may be suspended.

Requirements of a University Merchant

All University Merchants and their designated staff must adhere to the following requirements.

- Phone order card payments must be processed in a secure area. All employees and students working in the secure area, whether or not they are working specifically with Payment Card processing, must undergo a background check.
- University Merchants may not process Payment Cards or Cardholder Data for other units or departments.
- Prior to acquiring or using a Payment Card system, approval is needed from the Information Security Officer and all contracts, including vendor agreements, are required to be reviewed by the Office of General Counsel.
- Third-party processors and payment gateways must provide evidence of and maintain continued compliance with the most recently published PCI-DSS for the duration of relationship with the University. Evidence from the Acquiring Bank is to be retained by the Information Security Officer.
- Payment Card and Cardholder Data are prohibited from being processed through University Information Resources and must be processed only through approved third -party PCI-DSS compliant payment processing resources.
- University Merchants may not request or submit cardholder information via email or other non-secure means.
- University Merchants who receive unsolicited Payment Card/Cardholder Data information should immediately notify the sender and advise the sender of an appropriate way to make payment. Cardholder information should NOT be re-transmitted in any response and the unsolicited data must be securely deleted and/or shredded immediately.

Waivers and Exceptions

Departments subject to the mandatory requirements or standards set forth in this policy may request through the Controller's Office a waiver or exception from a particular requirement or standard that cannot practicably be followed without substantial operational hardship or excessive cost. Any waiver or exception must be documented through the Controller's Office and are required to be reviewed and approved by Information Security Officer and Office of General Counsel. The waiver or exception may be granted provided that waiver or exception would not result in a violation of applicable law or regulation.

Reporting a Data Breach

Any known or suspected breach in Payment Card or Cardholder Data should immediately be reported to securityincident@suffolk.edu and follow the Incident Response Policy.

Violation of Policy

The University reserves the right to monitor network traffic, perform random audits, and to take other steps to insure the integrity of its information and compliance with this Policy. Violations of this Policy may lead to appropriate disciplinary action, which may include temporary or permanent restrictions on access to certain information or networks. Willful or repeated violations of this Policy may result in dismissal from the University.

Revision History

Version	Date	Responsible University Office	Approved By
1.0	04/22/2014	Office of Controller - Official Controller	Senior VP Danielle Manning