MERCHANT SERVICES - Policy for Acceptance and PCI-DSS Compliance

I. BACKGROUND:

The Payment Card Industry (including VISA, Master Card, AMEX, and Discover) has established important and stringent security requirements to protect credit card data. These are called the PCI Data Security Standards or "PCI-DSS." These standards include controls for handling and restricting credit card information, computer and internet security, and reporting of a breach of credit card information.

II. PURPOSE:

This policy defines the steps that personnel responsible for Merchant Services accounts at Rensselaer must use to access and secure payment card data in paper and electronic form. It also establishes responsibility for all steps in the processing of payment card data, self-assessment of the merchant account and remediation of processes associated with the transmission, storage or processing of payment card data.

All Rensselaer personnel responsible for merchant service processing must complete an annual self-assessment survey which is submitted to the Assistant Treasurer's Office.

III. SCOPE AND ENFORCEMENT:

This policy applies to all personnel of Rensselaer while performing Institute employment duties, including student employees. Employees who violate the requirements of this policy are subject to disciplinary action, including termination of employment.

IV. DEFINITIONS:

Credit Card Information: The full magnetic stripe or the PAN (Primary Account Number) plus any of the following: Cardholder name, Expiration Date or Service Code.

Department Responsible Person ("DRP"): That person designated by a Rensselaer department as having primary authority and responsibility for merchant service processing within that department. A DRP must, at a minimum, hold the title of Business Administrator within the department where they have merchant service processing responsibility.

Merchant Services: The buying and selling of products or services over electronic systems such as the internet and other computer networks using MasterCard, Visa, AMEX or Discover as a payment method.

Payment Card Merchants: A relationship set up by the Assistant Treasurer's office between a Rensselaer department or other entity and a bank in order to accept payment card transactions.

Self-Assessment: The PCI Self-Assessment Questionnaire (SAQ) is a validation tool that is primarily used by merchants to demonstrate compliance to the PCI DSS.

V. PROCESS:

Any Rensselaer department accepting payment card and/or electronic payments for gifts, goods or services must designate a Department Responsible Person ("DRP").

All Department Responsible Persons must:

1. Ensure that all employees, contractors and agents with access to payment card data within the department acknowledge on an annual basis and in writing (the form is located at the end of this policy) that they have read and understood this document (Merchant Services – Policy for Acceptance and PCI-DSS Compliance). The acknowledgements must be submitted to the Assistant Treasurer's Office on an annual basis.

2. All DRP's and all employees with access to payment card data must ensure that all Credit Card Information stored, processed or transmitted by the department in the course of performing Institute business, regardless of how the payment card data are stored (physically or electronically, including but not limited to account numbers, card imprints, and Terminal Identification Number (TIDs)) is collected in a way that meets all PCI-DSS compliance requirements. Data is considered to be secured only if the following criteria are met:
    - Only those with the need-to-know are granted access to payment card and electronic payment data.
    - Email should not be used to transmit payment card or personal payment information. If it should be necessary to transmit payment card information, only the last four digits of the payment card number can be displayed.
    - Payment card or personal payment information is never downloaded onto any portable devices such as USB flash drives, compact disks, laptop computers or personal digital assistants
    - Fax transmissions (both sending and receiving) of payment card and electronic payment information can only be on those fax machines whose access is restricted to only those individuals who must have contact with payment card information in order to do their jobs.
    - The processing and storage of personally identifiable credit card or payment information beyond the period of time necessary for normal business operations to occur (typically intra-day) on Rensselaer's computers and servers is prohibited.
    - Only secure communication protocols and/or encrypted connections to the Authorized Vendor are used during the processing of Merchant Services transactions.
    - The three-digit card-validation code printed on the signature panel of the payment card ("CVV Code") is never stored in any form. In the case of American Express, this is a four digit code on the front of the credit card.
    - The full contents on any track from the magnetic stripe (on the back of a payment card, in a chip, etc) are never stored in any form
    - All but the first and the last four digits of any payment card account number are always masked if it is necessary to display payment card data
    - All media containing payment card or personal payment data that are no longer needed are destroyed or made unreadable.

No Rensselaer employee, contractor or agent who obtains access to payment card or other personal payment information in the course of conducting business on behalf of the Institute may sell, purchase, provide, share, or exchange said information in any form including but not limited to imprinted sales slips, carbon copies of imprinted sales slips, mailing lists, tapes, or other media obtained by reason of a card transaction to any third party other than to the Institute's, depository bank, Visa, MasterCard or other credit card company, or pursuant to a government request. All requests to provide information to any party outside of the department must be coordinated with the Assistant Treasurer's Office.

Departments must use an approved processor to process all Merchant Services transactions. If a department believes that it has a significant business case or processing requirement that cannot be achieved using the services of an approved processor and wishes to utilize an alternative, the DRP must initiate the request to the Assistant Treasurer's Office for a release from the approved processor

requirements specified by this policy. Only the Assistant Treasurer's Office and the Information Security Director together may authorize the adoption of alternative Merchant Services vendors and products.

In the event that the Assistant Treasurer's Office and the Information Security Director authorize the use of an alternative Merchant Services vendor, then the following must occur:

1. The DRP must provide proof that the alternate Merchant Services vendor is certified PCI compliant and ensure that the department and its vendor comply with all relevant provisions of this document (Merchant Services – Policy for Acceptance and PCI-DSS Compliance

Establishing a New Merchant Account

A department that wants to accept credit card payments should contact the Assistant Treasurer's Office to complete a request for a Merchant Services Account Form.

Responding to a Security Breach

In the event of an actual, possible or suspected breach, the DRP must immediately contact the Assistant Treasurers office as well as the Information Security Director. In addition, the department must immediately execute each of the additional relevant steps detailed below.

- The DRP or any individual suspecting a security breach involving Merchant Services transactions must immediately ensure that the following steps, where relevant, are taken to contain and limit the exposure of the breach:
    a. Prevent any further access to or alteration of the compromised system(s) (i.e. do not log on at all to the machine and/or change passwords.)
    b. Do not switch off the compromised machine; instead, isolate the compromised system(s) from the network by unplugging the network connection cable.
    c. Preserve logs and electronic evidence.
    d. Log all actions taken.

- The Assistant Treasurer's Office shall alert the processor of the suspected breach

APPENDIX A

The intent of the Assistant Treasurer's office is to minimize the number of vendors that handle credit card data on behalf of Rensselaer. The following vendors and their associated processing formats have been approved for use by specific merchant accounts and have PCI compliant language in their contract or in an amendment of their contract.

Payment Processors

- CyberSource
- Paymentech

Application Vendors

- Paypal
- Arts Management Theatre Manager
- Blackboard Transact
- Radiant Counterpoint

PAYMENT CARD INDUSTRY – DATA SECURITY STANDARD (PCI-DSS) POLICY ATTESTATION

Department:	
Merchant ID*:	
Department Responsible Person:	

I have read and acknowledged the following the following Institute process:

MERCHANT SERVICES - Policy for Acceptance and PCI-DSS Compliance

Last Name: _____

First Name: _____

Signature: _____

Date: _____

Affirmation that you read and understand this policy and that as a Rensselaer employee you agree to adhere to them. PCI Requirement 12.6.2 requires employees to acknowledge in writing that they have read and understand the company's security policy and procedure.

Instructions:

1. Review and update department processes.
2. Provide a form for each person who processes credit card transactions in your department.
3. Return completed forms to the Assistant Treasurer's Office.