CORNELL UNIVERSITY
POLICY LIBRARY

Accepting Credit Cards to Conduct University Business

POLICY 3.17

Volume: 3, Financial Management
Chapter: 17, Accepting Credit Cards to Conduct University Business
Responsible Executive: Vice President for Financial Affairs and University Treasurer
Responsible Office: Office of the Treasurer
Originally Issued: January 2001
Last Full Review: Juy 13, 2018
Last Updated: July 13, 2018

POLICY STATEMENT

For all units that accept credit cards as a method of payment for goods or services in relation to university business/operations, Cornell University requires compliance with Payment Card Industry – Data Security Standards (PCI-DSS) protocols, and with the procedures outlined in this document. Units wishing to accept credit cards for payment must be pre-approved by the Office of Cash Management (Ithaca campus units) or the Finance Office (Weill Cornell Medicine Units).

REASON FOR POLICY

The university strives to ensure proper stewardship of its assets while supporting its mission; toward this end, all units must treat the acceptance of credit cards in a consistent and efficient manner.

ENTITIES AFFECTED BY THIS POLICY

☑ Ithaca-based campuses and locations

☑ Cornell Tech campus

☑ Weill Cornell Medicine campuses

WHO SHOULD READ THIS POLICY

- Individuals responsible for accepting credit cards to conduct university business
- Individuals responsible for developing or maintaining technology to conduct credit card transactions
- Individuals utilizing third-party solutions to process credit card transactions for university business

WEB ADDRESS FOR THIS POLICY

- This policy: www.dfa.cornell.edu/policy/policies/accepting-credit-cards-conduct-university-business
- University Policy Office: www.policy.cornell.edu

Cornell Policy Library
Volume: 3, Financial Management
Responsible Executive: Vice President for Financial Affairs and University Treasurer
Responsible Office: Office of the Treasurer
Originally Issued: January 2001
Last Full Review: July 13, 2018
Last Updated: July 13, 2018

POLICY 3.17

Accepting Credit Cards to Conduct University Business

CONTENTS

CONTENTS, continued

POLICY 3.17

Accepting Credit Cards to Conduct University Business

RELATED RESOURCES

University Policies and Documents Applicable to All Units of the University

University Policy 3.1, Accepting University Gifts

University Policy 3.6, Financial Irregularities, Reporting and Investigation

University Policy 3.20, Cost Transfers on Sponsored Agreements

University Policy 3.22, Safekeeping of Financial Assets, Including Cash, Checks, and Securities

University Policy 3.25, Procurement of Goods and Services

University Policy 4.2, Transaction Authority and Payment Approval

University Policy 4.7, Retention of University Records

University Policy 5.1, Responsible Use of Information Technology Resources

University Policy 5.10, Information Security

University Policies and Documents Applicable to Only Ithaca Campus Units

University Policy 3.2, Travel Expenses

University Policy 4.3, Sales Activities on Campus

University Policy 4.12, Data Stewardship and Custodianship

University Policy 5.3, Use of Escrowed Encryption Keys

University Policy 5.4.1, Security of Information Technology Resources

University Policy 5.4.2, Reporting Electronic Security Incidents

Cornell's PCI Incident Response Plan

Policies and Documents Applicable to Only Weill Cornell Campus Units

University Policy 3.2.1, Travel

WCM Policy 12.5, PCI Policy

External Documentation

PCI Security Standards Council

PCI Security Standards Council List of Validated Payment Applications

University Forms and Systems

Ithaca Campus Units	*Weill Cornell Campus Units*
Application for Credit Card Merchant Accounts	myCertificates (Security Awareness Training)
Credit Card Awareness Training	WCM File Transfer Service
PCI Self-Assessment Questionnaire (SAQ) Guidelines and Documents	Unit Training Attestation

POLICY 3.17

Accepting Credit Cards to Conduct University Business

CONTACTS

Direct any general questions about this policy to your college or unit administrative office. If you have questions about specific issues, contact the following offices.

Contacts, Ithaca Campus Units

Subject	Contact	Telephone	Email/Web Address
Policy Clarification	Cash Management	(607) 254-1590	cashmanagement@cornell.edu
Breach, Reporting	Cash Management	(607) 254-1590	cashmanagement@cornell.edu
	IT Security Office	(607) 255-6664	pci-help@cornell.edu
Contracts with Third-Party Providers	Procurement and Payment Services	(607) 255-3804	procurement@cornell.edu www.dfa.cornell.edu/procurement/
Departmental Journal Credit	Cash Management	(607) 254-1590	cashmanagement@cornell.edu
General Credit Card – Related Questions	Cash Management	(607) 254-1590	cashmanagement@cornell.edu
Credit Card Processor Support Lines	FreedomPay	(877) 888-8430	
	Elavon	(800) 725-1245 (available 24/7)	
PCI Compliance, Technical or Security	IT Security Office	(607) 255-6664	pci-help@cornell.edu
Sales Tax and Other Tax Issues	University Tax Office	(607) 255-5195	tax@cornell.edu www.dfa.cornell.edu/tax/

CONTACTS, WEILL CORNELL CAMPUS UNITS

Contacts, Weill Cornell Campus Units

Subject	Contact	Telephone	Email/Web Address
Policy Clarification			
Breach, Reporting a	Privacy Office	(212) 746-1121	privacy@med.cornell.edu
	Information Security	(646) 962-3010	its-security@med.cornell.edu
Contracts with Third-Party Providers	Office of University Counsel	(212) 746-0463	jkahn@med.cornell.edu
PCI Compliance, Business Practices	Privacy Office	(212) 746-1121	privacy@med.cornell.edu
	Controller, Finance	(646) 962-3635	jos2067@med.cornell.edu
PCI Compliance, Technical or Security Issues	Information Security	(646) 962-3010	its-security@med.cornell.edu
Sales Tax or Unrelated Business Income Issues	Finance Department Compliance Office	(646) 962-3695	pat2005@med.cornell.edu

DEFINITIONS

These definitions apply to terms as they are used in this policy.

Acquirer	The bank or financial institution that accepts credit and or debit card payments for products or services on behalf of a merchant. The term acquirer indicates that the bank accepts or acquires transactions performed using a credit card issued by all banks within the card industry.
Bank	A financial institution that provides merchant accounts to enable a unit to accept credit card payments. Funds are deposited into an account established at this institution.
Breach	Also called "data breach." An incident wherein information is stolen or taken from a system without the knowledge or authorization of the system's owner. Stolen data may involve sensitive, proprietary, or confidential information, such as credit card numbers, customer data, trade secrets or matters of national security.
Card Verification Code or Value	A data element on a card's magnetic stripe that uses secure cryptographic process to protect data integrity on the stripe, and reveals any alteration or counterfeiting. Referred to as the following, depending on payment card brand: • CAV – Card Authentication Value – JCB • CVC – Card Validation Code – MasterCard • CVV – Card Verification Value – Visa and Discover • CSC – Card Security Code – American Express (AMEX) Also, the rightmost three-digit value printed in the signature panel area on the back of the card (for Discover, Visa, MasterCard) or the four-digit number printed above the primary account number (PAN) on the face of the card (for AMEX). • CID – Card Identification Number – AMEX and Discover • CAV2 – Card Authentication Value 2 – JCB • CVC2 – Card Validation Code 2 – MasterCard • CVV2 – Card Verification Value 2 – Visa
Chargeback	The deduction of a disputed sale previously credited to a unit's account when the unit fails to prove that the customer authorized the credit card transaction.
Confidential Information	Also called "Level 1 Information." Information that has been determined by institutional information stewards to require the highest level of privacy and security controls. Currently, any information that contains any of the following data elements, when appearing in conjunction with an individual's name or other identifier, is considered to be confidential (level 1) information: • Social Security number • Credit card number • Driver's license number • Bank account number • Protected health information, as defined in the Health Insurance Portability and Accountability Act (HIPAA)
Credit Card Advisory Group (C-CAG)	A group of individuals that works with campus stakeholders to identify necessary compliance activities or technology solutions, recommends updates to this and other policies, and advises the

DEFINITIONS, continued

	executive vice president and chief financial officer on PCI requirements.
Customer	An individual or other entity that makes a payment to the university for goods or services.
e-Commerce	Business transactions that are conducted via the Internet. For the purposes of this policy, e-Commerce refers to credit card transactions that are made online.
Data Breach	See "*Breach*."
Lockbox Processing	A method of processing through a **lockbox** is a service offered by commercial banks to organizations that simplifies collection and **processing** of account receivables by having those organizations' customers' payments mailed directly to a location accessible by the bank. See Table 1, Methods of Processing Transactions, in the Procedures, Ithaca Campus Units section of this policy.
Merchant	A unit that accepts credit cards as a method of payment.
Merchant Discount	A percent or per-transaction fee that is deducted from the unit's gross credit card receipts and paid to the bank.
Merchant ID (MID)	An account established for a unit by a bank to credit sale amounts and debit processing fees.
Merchant Fee	A percent and/or per-transaction fee that is deducted monthly from the unit's gross credit card receipts and paid to the bank. Fees typically encompass service fees, discounts and interchange fees passed along from Visa/MasterCard.
P2PE	Point-to-point encryption. A standard created by the Payment Card Industry Security Standards Council (PCI SSC) in which credit card data is encrypted immediately upon swiping/dipping the card at the terminal and remains encrypted until it reaches the processor. Devices must be reviewed and approved by the PCI SSC before they can be listed as PCI-validated P2PE devices.
Payment Card Industry Data Security Standards (PCI DSS)	A set of comprehensive requirements for enhancing payment account data security, developed by the PCI SSC to help facilitate the broad adoption of consistent data security measures on a global basis.
PCI DSS Security Awareness Training	An online training program, available through CULearn for Ithaca campus units, and through myCertificates for Weill Cornell Medicine (WCM) campus units, that includes information on compliant processes (business and technical) and changes in industry standards.
PCI Security Standards Council (PCI SSC)	An organization for the ongoing development, enhancement, storage, dissemination, and implementation of security standards for account data protection in the payment card industry, through education and awareness. The organization was founded by American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc.
Personal Identification Number (PIN)	A numeric password known only to the user and a system to authenticate the user to the system.
POS	Point-of-sale device. A device that is used by a customer or the cashier to process a credit card payment.
Primary Account Number (PAN)	The 16-digit (15-digit for AMEX) account number on the credit card.

DEFINITIONS, continued

Report on Compliance (ROC)	An annual certification report issued by the PCI SSC to a third-party provider that has been validated as PCI-compliant.
Self-Assessment Questionnaire (SAQ)	A form used as self-validation tool to assist merchants and service providers in evaluating their compliance with PCI Data Security Standards (PCI DSS). For more information, contact Cash Management. Consult PCI SSC for the appropriate SAQ. See Related Resources.
Terminal and Printer	A method of processing credit cards at the university. See Table 1, Methods of Processing Transactions, in the Procedures, Ithaca Campus Units section of this policy.
Unit	A college, department, program, research center, business service center, office, or other operating unit.

RESPONSIBILITIES, ITHACA CAMPUS UNITS

The following are the major responsibilities each party has in connection with this policy.

Cash Management	Negotiate all contracts with credit card companies. Review requests for new merchant IDs (MIDs), and establish where appropriate. Consult with units regarding merchant accounts, merchant discounts, and all other aspects of this policy. Keep current with Payment Card Industry Data Security Standards (PCI DSS) regulations and make changes to processes, as appropriate. Coordinate and account for annual PCI DSS requirements: • Provide PCI security awareness training portal to units. • Collect, from every unit, signed and dated attestations that all appropriate individuals have completed the annual security awareness training. o Review unit Self-Assessment Questionnaire (SAQ) completion status; collaboratively work with units that have an incomplete/fail status toward a successful completion of this requirement. • Coordinate and review quarterly scans. • Confirm that units using third-party providers have submitted proper documentation. o Submit annually the necessary documentation to acquirer for PCI certification at the university level.
Cornell IT Security Office (ITSO)	Maintain security standards as required by this policy. Keep current with PCI DSS regulations and make changes to tools and processes, as appropriate. Consult with units on technical PCI DSS issues. Assist units when there are data breaches. Assist Cash Management in its mandatory annual training sessions.
Credit Card Advisory Group (C-CAG)	Work with campus stakeholders to identify necessary PCI compliance activities or technology solutions in compliance with the latest laws and standards. Recommend updates to this and other policies related to accepting credit card payments in compliance with the latest laws and standards. Advise the executive vice president and chief financial officer and other leadership stakeholders on PCI requirements, business needs, and compliance objectives.
Cornell Procurement and Payment Services	Consult with units regarding service contracts for third-party outsourcing of PCI-compliant credit card processing systems. When evaluating contracts on behalf of units, verify that the contract states that it will become null and void if the vendor does not maintain PCI DSS compliance.
Individual	Report any breaches to the IT Security Office and Cash Management, according to the "*Reporting Breaches*" section of this policy.
Senior Finance Officer or Designee	Attest annually to Cash Management confirming unit's completion of the PCI security awareness training requirement. Approve (by signing a form) all applications for new MID requests.

POLICY 3.17

Accepting Credit Cards to Conduct University Business

RESPONSIBILITIES, ITHACA CAMPUS UNITS, continued

Unit Processing Payments	Determine whether accepting credit cards will benefit the unit and whether there is a valid business purpose. **Applying for a Merchant ID (MID)** Submit to the senior finance officer or designee for approval a completed application for a new MID. Once approved by the senior finance officer or designee, submit approved MID application to Cash Management. **Administering the Credit Card Process** Maintain security standards and employ procedures as required by this policy, no matter what type of credit card processing is utilized. Provide proper unit controls regarding who may process credit card transactions (e.g., terminal passwords may be established for return transactions). Maintain a segregation of duties between employees who process credit card transactions, those who reconcile daily batches, and those who post to the general ledger. Charge sales tax where appropriate. Annually complete a merchant SAQ. (See Related Resources.) **Taking Credit Card Payments** Get an authorization from the bank for every transaction. Validate that the signature on the card reasonably matches the signature of the purchaser. If the card says “see Photo ID” - validate that the photo ID matches the name on the card of the purchaser. Accept credit cards only for sales that are not prohibited (see the Prohibited Credit Card Activities segment of this document). Complete an annual PCI self-assessment questionnaire, and submit it to Cash Management. (See Related Resources.) Ensure that anyone responsible for and/or involved with credit card processing (sales, reconciliation, management of these individuals, technical support) attests to having taken the annual PCI DSS Security Awareness Training, and being fully trained and apprised of unit and university policies and procedures for handling credit card transactions. Submit to Cash Management a signed and dated attestation that this requirement was met. Charge sales tax where appropriate. **When a Card is not Present (e.g., Telephone Payment or Order Form)** Obtain the expiration date for use in the authorization process. Obtain an authorization from the bank for every transaction. Retain a copy of the confirmation. Destroy the card number after process completion with a cross-cut shredder. **Handling Transactions after the Sale** Balance and transmit transactions to the bank daily, if using a terminal. Complete and submit an electronic journal as part of the batch closing process. Keep copies of credit card receipts and journal/register tapes. Store them as securely as you would any confidential information. After a retention period of six months, destroy them with a cross-cut shredder.

POLICY 3.17

Accepting Credit Cards to Conduct University Business

RESPONSIBILITIES, ITHACA CAMPUS UNITS, continued

	Reconcile the monthly credit card statement with the general ledger (KFS) within 30 calendar days of the receipt of the statement.
	Respond to all disputed charges, in writing, within two business days of the receipt of the notice.
	Process refunds according to this policy.
	Reconcile internal sales records to the Kuali Financial System (KFS).
	If Using Third-Party Outsourcing
	Consult with Procurement and Payment Services before signing a service contract.
	Annually attach a Report on Compliance (ROC), validating PCI DSS compliance of any third-party provider with your completed SAQ.

POLICY 3.17

Accepting Credit Cards to Conduct University Business

RESPONSIBILITIES, WEILL CORNELL CAMPUS UNITS

The following are the major responsibilities each party has in connection with this policy.

Individual	Record Retention Keep copies of credit card receipts and related documents. Store them as securely as you would any confidential information. Destroy records after six months. Send all supporting documents to Finance promptly. Disputed Charges and Refunds Respond to all disputed charges, in writing, within two business days of the receipt of the notice. Process refunds according to this policy.
Director of Security, Identity, & IT Business Continuity	Maintain security standards as required by this policy and ITS policy 12.5 – PCI Policy. Keep current with PCI DSS regulations and make changes to tools, processes, and the ITS PCI policy, as appropriate. Assist with providing adequate training content for individuals processing credit card transactions. Consult, advise, and perform risk assessments pertaining to technical PCI DSS issues or when onboarding new merchants. Assist with incident response, including activation of the Security & Privacy Incident Response Plan, as needed.
Unit	Institute proper controls regarding who may process credit card transactions. Monitor adherence to this policy. Maintain a segregation of duties between employees who process credit card transactions, those who reconcile daily batches, and those who post to the general ledger. Complete an annual PCI self-assessment questionnaire (SAQ). (See Related Resources.) **At Point of Sale, When a Card is Presented** Check the signature on the card and compare it to that of the person paying for the service or making the donation. Check the expiration date on the card to make certain that the card is valid. Process the payment and obtain a confirmation (authorization number) from the bank for every transaction. Accept credit cards only for purchases that are not prohibited (see the Prohibited Credit Card Activities segment of this document). Post payments in a timely manner. **At Point of Sale, When Only a Card Number is Provided (Telephone Payment)** Process the payment and obtain a confirmation (authorization number) from the bank for every transaction. Retain a copy of the confirmation. Post payments in a timely manner. Destroy any physical information after processing. **When a Third Party Processes a Payment** Obtain confirmation of the payment. Process the payments.

Cornell Policy Library
Volume: 3, Financial Management
Responsible Executive: Vice President for Financial Affairs and University Treasurer
Responsible Office: Office of the Treasurer
Originally Issued: January 2001
Last Full Review: July 13, 2018
Last Updated: July 13, 2018

POLICY 3.17

Accepting Credit Cards to Conduct University Business

PRINCIPLES

Introduction

A university unit that sells goods or services may choose to accept credit cards from its customers as a payment option. Credit cards may be accepted only for goods, services, non-degree course registration fees, and gifts to the university.

◆**Note:** This policy does not cover third party vendors selling goods or services on campus. For more information, see University Policy 4.3, Sales Activities on Campus.

Prohibited Credit Card Activities

Prohibited credit card activities include, but are not limited to:

- Tuition payment for a degree-granting program.

  ◆**Note:** Credit cards may be used to pay for non-degree courses.
- The disbursement of cash from the university, including cash advances and amounts over a sale amount, except for travel advances on corporate credit cards (for more information, see university policies 3.2 and 3.2.1, regarding university travel).
- Adjusting the price of goods or services based on the method of payment (e.g., giving a discount to a customer for paying with cash).

For more information, contact Cash Management (at Weill Cornell Medicine (WCM), contact the controller in the Finance Department).

Overall responsibility for a unit's credit card system rests with the unit's senior finance officer.

◆ **Caution**: Your unit should not accept credit cards unless there is a valid business need. When considering accepting credit cards, contact Cash Management.

◆**Note:** A unit that sells goods and services, irrespective of the method of payment, must evaluate whether the sale requires the collection of sales tax and/or the reporting of unrelated business income. Contact the University Tax Office, (or, at WCM, the Finance Department Compliance Office), for additional guidance.

Credit Card Advisory Group (C-CAG)

The Credit Card Advisory Group (C-CAG) serves as a resource for campus stakeholders for identifying necessary compliance activities or technology solutions and reviews and recommends updates to this and other policies related to credit card payment processing, in compliance with the latest laws and standards. C-CAG also advises the executive vice president and chief financial officer and other leadership stakeholders on PCI requirements, business needs, and compliance objectives.

POLICY 3.17

Accepting Credit Cards to Conduct University Business

PRINCIPLES, continued

PCI DSS Compliance

The credit card industry has developed technical and business standards that affect the way in which credit card business is conducted, called "Payment Card Industry Data Security Standards" (PCI DSS) (www.pcisecuritystandards.org).

Cornell has developed PCI-compliant procedures for every method of payment processing at Cornell. Every entity engaged in processing credit card transactions must comply with this structure. Prior to accepting credit cards, the unit must consult with Cash Management (at WCM, the Assistant Controller in the Finance Department) to determine the most efficient and secure processing method that meets unit business needs within the centrally developed processing structure.

Acceptable Credit Cards

For Ithaca campus units, please check the Treasurer's website for information.

In WCM units, the university currently accepts Visa, MasterCard, Discover, and American Express.

◆**Caution:** Units are prohibited from negotiating their own contracts with credit card companies or third-party vendors. For more information, contact Cash Management (at WCM, contact the controller in the Finance Department).

Security and Technical Standards

All processes, procedures, or technologies must meet the required security standards outlined in the "Payment Card Industry Data Security Standards" (PCI DSS). Prior to implementation, the office of Cash Management (at WCM, the Finance Department) and the IT Security Office (ITSO) (at WCM, Information Technologies and Services (ITS)) must evaluate and approve any process, procedure, or technology used.

Units will work in conjunction with Cash Management and CIT (at WCM, with the Finance Department and ITS) to create and maintain a PCI-compliant environment for all systems involved in credit card processing.

Standards for Business Processes, Paper and Electronic Processing

Standard business processes and practices must adhere to PCI DSS requirements at all times.

Methods of Processing Transactions

There are three accepted methods for processing transactions: Card present, e-Commerce, and mail order – lockbox/telephone order. For details on each of the methods, see Table 1, Methods of Processing Transactions, which follows.

◆**Caution:** Do not process any transaction using cardholder information transmitted via email. If you receive credit card information via email, delete the email, and **do not process the transaction**. Instruct the customer of this provision.

POLICY 3.17

Accepting Credit Cards to Conduct University Business

PRINCIPLES, continued

Table 1

Methods of Processing Transactions

Method	Description	Sending Transactions to the Bank
Lockbox Processing	This is the required method for credit card orders received through the United States Postal Service. Customers are directed to send orders to a specific U.S. post office box. The bank or caging and keying company removes materials each day, processes the credit card information, and credits accounts according to the units' specific directions. The credit card material is returned to the unit, as a PDF file, on the same business day.	The bank or caging and keying company is responsible for processing credit card receipts on a daily basis and crediting the unit account. The unit is required to design forms that allow the PAN, CVC2 et al., and expiration date to be removed easily for immediate shredding after processing by bank personnel.
PC Processing	The unit must purchase the required tool (contact Cash Management, or, at WCM, the Finance Department). The PC that is processing credit cards must: • Be a stand-alone machine (no Web surfing or other activities permitted). • Connect to the Ithaca Cornell or WCM PCI DSS-compliant infrastructure.	
e-Commerce	e-Commerce – web-hosted applications must be compliant and vetted through Cash Management and the ITSO.	Transactions are sent automatically via the payment processing service.
Terminal and Printer (includes standalone and POS devices)	The unit purchases a P2PE terminal, and printer if necessary (through Cash Management or, at WCM, through the Finance Department), which are connected to analog telephone lines, Wi-Fi, or a broadband network. The unit swipes/dips the customer credit card to obtain authorization for the transaction. A receipt is printed, which the customer signs. Merchant receipts should be secured in a locked, limited-access place. ◆**Caution:** If a terminal is IP-enabled, it must reside on the Ithaca-Cornell or WCM ITS PCI-compliant network and related infrastructure.	The day's receipts must be balanced and transmitted to the bank daily if there is one transaction or more. No transmittal is required if there are no transactions. No transmission equates to no sale. After 10 days, the sale is void. Each additional day of non-transmittal of data results in a higher discount fee charged to the unit.

POLICY 3.17

Accepting Credit Cards to Conduct University Business

PROCEDURES, ITHACA CAMPUS UNITS

Requirements for Individuals Involved with Credit Card Processing

The following actions are required, and are the shared responsibility of those involved in credit card sales and reconciliation, those who manage these individuals, and technical support staff.

1. Complete the annual Payment Card Industry Data Security Standards (PCI DSS) Security Awareness Training (see Related Resources).
2. Submit to Cash Management a date attestation that this requirement is met, signed by your unit's senior finance officer (see Related Resources).

Posting and Reconciling Transactions

Using the general ledger account information provided in the merchant ID (MID) application, Cash Management will record credit card revenue and chargebacks to department accounts on a daily basis and will also post the merchant fees for each MID on a monthly basis. Units will post daily sales transactions.

Units are expected to reconcile internal records of sales activity to the designated general ledger account. The person(s) responsible for reconciliation should not have access to the sales processing system. If there is more than one category for either internal or external sales, the designated general ledger account becomes a clearing account, and the unit must distribute sales activity and "zero" these accounts via a KFS Distribution of Income and Expense (DI) e-doc. Contact Cash Management for additional information.

Accepting University Procurement Cards

On your credit card sales deposit, code credit card sales made to non-procurement card users as external revenue, and credit card sales made to procurement card users as interdepartmental revenue. This entry into the general ledger is performed automatically by Cash Management, if an internal merchant account has been established. For more information, contact Cash Management.

◆**Caution:** Evaluate whether you should collect sales tax on external sales; do not charge sales tax on interdepartmental sales. For more information, contact the University Tax Office at tax@cornell.edu.

Handling a Customer Disputed Charge

The bank is obligated to advise the unit, in writing, of a disputed charge. The unit is responsible to provide the bank with written proof that the transaction was authorized by the customer. Failure to respond or provide a copy of a receipt signed by the customer or documentation of the shipping address will result in a chargeback to the unit's account. All bank requests for information concerning a dispute must be answered within two business days of receipt.

POLICY 3.17

Accepting Credit Cards to Conduct University Business

PROCEDURES, ITHACA CAMPUS UNITS, continued

Processing Refunds

To process a refund, follow the procedure appropriate to the mode of processing.

When an item or service is purchased using a credit card and a refund is necessary, the refund must be credited to the same account from which the purchase was made, unless the original credit card account has been cancelled, in which case the refund may be issued to a different credit card. In addition, documentation of the original charge must be included with any refund transaction processed by the unit.

◆**Caution:** Under no circumstance is it permissible to issue a cash refund.

◆**Note:** For issuing a refund using the lockbox method, use a "Lockbox Credit Card Refund Form" (see Related Resources).

Outsourcing to Third-Parties

Units that outsource (to third-party service providers) the storage, processing, or transmission of cardholder data must obtain from them, annually, a Report on Compliance (ROC), which is evidence of a successfully completed PCI DSS assessment. This documentation must be submitted to Cash Management.

In addition, a unit (a) considering third-party outsourcing for credit card processing, or (b) renewing its current service contract must consult with Procurement and Payment Services, before signing the contract. Procurement and Payment Services will review the contract.

◆**Caution:** Units are prohibited from engaging third-party service providers that are not PCI-compliant and have not provided ROCs.

◆**Note:** Units are responsible for transaction reconciliation and general ledger entries for third-party transactions.

Canceling a Merchant ID

Should a unit decide that an MID is no longer needed, the unit must contact Cash Management to cancel the MID.

Decommissioning Computer Systems and Electronic Media Devices

When decommissioning a system that was part of a cardholder data environment, consult with the IT Security Office (ITSO) for proper disposal.

Actions if You Suspect a Breach

Units are required to notify the office of Cash Management (607-254-1590) and the IT Security Office (607-255-6664) immediately, upon suspicion of a breach. University Policy 5.4.2, Reporting Electronic Security Incidents, outlines more in-depth responsibilities and actionable next steps (see Related Resources).

POLICY 3.17

Accepting Credit Cards to Conduct University Business

PROCEDURES, ITHACA CAMPUS UNITS, continued

Requirements of the Individual

The most effective method to minimize the harm perpetrated in a breach situation is to take immediate action, in accordance with your unit's protocols. If you suspect or have a confirmed breach of credit card information, immediately contact Cash Management and the IT Security Office.

Also, the individual should perform the following technical tasks:

1. Do not access or alter compromised systems, (i.e., do not log on at all to the machine to change passwords or run antivirus software, and do not log in).
2. If using a wireless network, disable the wireless interface on the compromised system.
3. Do not turn the compromised machine off; instead, isolate compromised systems from the network, (i.e., unplug cable).

POLICY 3.17

Accepting Credit Cards to Conduct University Business

PROCEDURES, WEILL CORNELL CAMPUS UNITS

PCI DSS Compliance Certification

To document Payment Card Industry (PCI) compliance, the acquirer will issue an annual certification of PCI compliance when all Payment Card Industry Data Security Standards (PCI DSS) requirements are met. This certification must be submitted each year to the Office of Cash Management, at the Ithaca Campus, no later than June 30. This activity will be coordinated by the director of Security, Identity, & IT Business Continuity.

Training in PCI requirements is provided by the college based on job function.

Credit Card Information and Email

Do not use unsecured email to transmit cardholder information.

◆**Caution:** Instruct customers of this prohibition. Additionally, if a unit receives credit card information via unsecured email, the unit must delete the email, and not process the transaction, notifying the customer.

◆**Note:** Anyone transmitting sensitive electronic information may do so using the WCM File Transfer Service or encrypted email (#encrypt).

For more information, please visit http://its.weill.cornell.edu/services/email-calendar/encrypted-email.

Establishing a Merchant Account

To establish a merchant account, contact the controller.

Decommissioning Computer Systems and Electronic Media Devices

When a computer system or media device that was used for credit card processing is taken out of production, all sensitive data must be removed. The hard drive of any computer system or any media device must be completely wiped and overwritten per instructions provided by ITS.

At the very least, the media device must be erased and zeroed utilizing the United States Department of Defense 5220.22-M short-wipe procedure. A media device can be re-commissioned only after it has been completely sanitized. If a media device will not be re-commissioned, it must be physically destroyed. Contact Environmental Health and Safety if a computer is to be destroyed.

Protecting Sensitive Information

Terminals, laptops, and other media devices that contain high-risk data, (as defined in WCM Policy 11.03 – Data Classification), must be identified and monitored.

Further, any individuals who regularly handle credit card information must protect that information as detailed in WCM Policy 12.2 – Physical Security and WCM Policy 12.5 – PCI Policy.

POLICY 3.17

Accepting Credit Cards to Conduct University Business

PROCEDURES, WEILL CORNELL CAMPUS UNITS, continued

Third-Party Outsourcing

Units that outsource storage, processing, or transmission of cardholder data to third-party providers must obtain from them annually, a Report on Compliance (ROC), which is evidence of a successfully completed PCI DSS assessment. This documentation must be submitted to the Controller.

In addition, units that are considering third-party outsourcing for credit card processing, or are renewing their current contracts, must consult with Office of University Counsel before signing a service contract. Office of University Counsel will review the contract for appropriate language, including a clause addressing continued compliance and specific terms regarding financial responsibility in the event of a breach.

◆**Caution:** Units are prohibited from engaging third-party service providers that are not PCI-compliant and have not provided ROCs.

Transaction Reconciliation

Finance will post the sales transactions from the bank daily, and discount and other fees monthly. Each unit is responsible to reconcile its internal sales records. The person(s) responsible for reconciliation should not have access to the sales processing system.

Processing Refunds

When an item or service is purchased using a credit card and a refund is necessary, the refund must be credited only to the same account from which the purchase was made, unless the original credit card account has been cancelled, in which case the refund may be issued to a different credit card. In addition, documentation of the original charge must be included with any refund transaction processed by the unit.

◆**Caution:** Under no circumstance is it permissible to issue a cash refund.

To process a refund, follow the procedure appropriate to the mode of processing.

Handling a Customer Disputed Charge

The bank is obligated to advise the unit, in writing, of a disputed charge. The unit is responsible to provide the bank with written proof that the transaction was authorized by the customer. Failure to respond or provide a copy of a receipt signed by the customer or documentation of the shipping address will result in a chargeback to the unit's account. All bank requests for information concerning a dispute must be answered within two business days of receipt.

Posting and Reconciling Transactions

It is important to record sales revenue accurately in the college's financial records. Units must submit to the controller the WCM fund(s) where the revenue from the credit card payments will be recorded.

PROCEDURES, WEILL CORNELL CAMPUS UNITS, continued

A unit is expected to reconcile internal records of sales activity to the designated fund.

Canceling a Merchant ID

Should a unit decide that a merchant ID (MID) is no longer needed, the unit must contact Finance to cancel the MID. Likewise, the associated processing method must be properly disabled (see the Decommissioning of Computer Systems and Electronic Media Devices segment of this policy).

Actions if You Suspect a Breach

Units must notify the Privacy Office and/or ITS Security when there is a suspected breach.

Requirements of the Individual

The most effective method to minimize the harm perpetrated in a breach situation is to take immediate action. If you suspect or have a confirmed breach of credit card information, immediately contact the Privacy Office, at (212) 746-1121, as well as ITS Security at (646) 962-3010.

Also, the individual should perform the following technical tasks:

4. Do not access or alter compromised systems, (i.e., do not log on at all to the machine to change passwords or run antivirus software, and do not log in).
5. If using a wireless network, disable the wireless interface on the compromised system.
6. Do not turn the compromised machine off; instead, isolate compromised systems from the network, (i.e., unplug cable).

POLICY 3.17

Accepting Credit Cards to Conduct University Business

INDEX

INDEX, continued