



Washington and Lee University

eCommerce Policy and Practices

Approved By: <u>Provost; Vice President for</u> <u>Finance and Administration / Treasurer</u>	Related Policies: <u>Information Security Program;</u> <u>Computing Resources, Network and Email Use</u> <u>Policy; and Confidentiality Policy</u>
History: Issued – <u>September 29, 2009</u> Revised – _____	_____
Responsible Office: <u>Business Office; ITS</u>	Additional References: _____

I. INTRODUCTION

Policy Statement

This policy provides direction on handling payment card and cardholder data at Washington and Lee University (“WLU”). Electronic commerce provides an expedient way to handle business transactions; however credit card industry regulations and general best practices require certain reasonable steps designed to protect the personal information and privacy of those who submit credit card information to the university.

Applicability

This policy applies to all departments, individuals, and organizations (as well as third parties, as particular subsections may be applicable) involved in the storing, processing, transmitting, or receiving of payment card or cardholder data at WLU.

II. 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.

Cardholder Data/Information – Cardholder data/information is any personally identifiable data associated with a cardholder’s account, including the account number, expiration date, name, address, or social security number.

eCommerce – eCommerce is an electronic transaction containing payment card and/or cardholder data.

Merchant – The acquiring bank contract with the merchant is informally referred to as a “merchant account.” The arrangement is in fact a line of credit and not a bank account. Under the contract, the acquiring bank exchanges funds with issuing banks on behalf of the merchant, and pays the merchant for the net balance of its daily payment card activity.

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

Payment System – A payment system is any application, system, or process that handles the payment card or cardholder data either electronically or manually.

WLU Merchant – A WLU department/office/organization that collects payments, electronically or manually, via credit card OR is otherwise involved in storing, processing, transmitting, or receiving payment card or cardholder data.

III. POLICY

A. Roles and Responsibilities

1) Information Security Program Committee

The Information Security Program Committee (“ISP”) was founded to oversee the security of the University’s non-public information through development and implementation of an overall Information Security Program. The Committee reports to the Provost and includes an administrator from each of the following offices and departments: Business, Financial Aid, Human Resources, Information Technology Services, Law School Records, Law School Technology, Student Affairs, University Advancement, University Registrar, and University Treasurer. In the context of eCommerce, the ISP Committee is responsible for:

- a) Coordinating contact with the University’s Public Communications representative
- b) Advising the Provost on the appropriate responsive action
- c) Implementing action(s) approved by the Provost
- d) General oversight of the eCommerce Committee

i) eCommerce Committee

The eCommerce Committee is a subcommittee of the ISP committee and was organized to educate University constituents about risks and exposures that the University faces as it collects, uses, shares and stores sensitive cardholder data. The eCommerce Committee’s goal is to improve understanding of privacy definitions and concepts drawn from laws, regulations, and best practices that affect eCommerce. The eCommerce Committee is responsible for:

- Proposing eCommerce procedures and policies (including amendments/edits) for adoption by appropriate senior level administrators;

- Creating and maintaining a list of University approved payment system products that meet PCI requirements;
- Revoking approved merchant status in accordance with this policy; and
- Acting as the ultimate approver of new University merchants and/or payment systems.

2) Controller's Office

The Controller's Office provides financial services to the campus. The office acts the single point of contact for financial eCommerce-related questions at WLU. The Controller's Office responsibilities include:

- a) Acting as the first point of contact for eCommerce related questions;
- b) Maintaining eCommerce contracts and merchant created self-governing policies;
- c) Acting as the first step for approval/denial of new merchants or payment systems;
- d) Coordinating contact with the acquiring bank(s) and/or payment brand(s);
- e) Approving new merchant accounts;
- f) Closing unauthorized merchant accounts;
- g) Maintaining financial guides as they pertain to acquiring merchant rates; and
- h) Serving on both the eCommerce Committee and the Information Security Program Committee.

3) Information Technology Services

Information Technology Services ("ITS") provides general technology services to the University such as email, network access, and phone/cable services. The Information Technology Services group in the context of eCommerce will be responsible for:

- a) Performing annual audits and security scans on WLU merchants;
- b) Issuing, renewing, and revoking user payment system passwords and accounts;
- c) Assisting in payment system configuration, which includes blocking users from administrative access where applicable;
- d) Applying system patches within one month of the patch becoming available for any system that processes or stores cardholder or payment card data.

i) Information Security Officer

The Information Security Officer ("ISO") is a staff member of ITS and develops, recommends, and monitors information security procedures at the University. The ISO also serves as a technical expert in information security policy issues for the University and periodically reports the effectiveness of information security controls to the University's Chief Technology Officer and/or Provost. As a member of the eCommerce

Committee, the ISO assists in the developing and implementing of eCommerce awareness programs. The ISO's responsibilities include:

- Serving on the Incident Response Team, the ISP Committee, and the eCommerce Committee;
- Auditing new payment systems prior to production and annually thereafter;
- Monitoring proper disposal of old data and password resets;
- Facilitating both new merchant and annual eCommerce training sessions; and
- Monitoring access to PCI systems, including logical access controls, server configuration and management, and logging and software patch management.

4) Office of General Counsel

The Office of General Counsel is responsible for providing legal representation, preventative legal advice and review, and legal opinions on substantive issues of law relating to University operations. With respect to eCommerce, the Office of General Counsel's responsibilities include:

- a) Providing advice/facilitation/oversight on statutory/regulatory compliance issues/programs and best practices;
- b) Representing the University in litigation;
- c) Engaging and supervising outside counsel, as appropriate;
- d) Reviewing eCommerce contracts;
- e) Advising the ISP Committee;
- f) Serving on the eCommerce Committee; and
- g) Reviewing and revising University policies, procedures, and handbooks, as appropriate.

5) Incident Response Team

The Incident Response Team ("IRT") responds to technology security issues that arise. The response can vary, depending upon the seriousness of the event, the risk of further or additional damage, and the type of coordination and notification required. When computer security incidents occur, the Incident Response Team will coordinate with the ISP Committee and handle all technology-based investigative and responsive actions. The Incident Response team's responsibilities include:

- a) Establishing incident response policy and procedures;
- b) Testing the incident response plan annually;
- c) Holding incident response training session annually with team members ;
- d) Providing annual review and familiarity with the business recovery and continuity plans
- e) Maintaining an incident response emergency team contact list of those members that are available 24/7;
- f) Notifying both the Office of General Counsel and the Chair of the University's ISP Committee of any breach/incident;

- g) Advising the ISP Committee on the nature of the breach/incident, possible courses of action, etc.;
- h) Maintaining data breach recordkeeping for breaches involving electronic data; and
- i) Performing preventive and predictive analysis to help mitigate against future threats.

B. Prior to Utilizing or Acquiring a Payment System

Prospective WLU Merchants and prospective third-party merchants should notify and obtain approval from the ISO prior to acquiring or utilizing a payment system. The Office of General Counsel should be contacted before any contract for a payment system is signed. To better understand PCI requirements, WLU merchants should review all four variations (A, B, C, and D) of the PCI DSS Self-Assessment Questionnaire (SAQ).

1) Setting up an eCommerce Bank Account

Bank accounts may only be opened with the University Treasurer's Office. Any bank account that has been established and has not been authorized by the University Treasurer's Office will be promptly closed by the University Treasurer's Office. The University Treasurer's Office approval is mandatory for payment card types, fee structures, and acceptable merchant rates. Typically, the following information is necessary to obtain lowest rates:

- a) Cardholder name;
- b) Account Number;
- c) Expiration date;
- d) Billing Address; and
- e) Phone number.

2) Systems hosted by an external merchant

All WLU merchants' third-party processors and payment gateways should provide evidence of Payment Card Industry Data Security Standards (PCI DSS) compliance with the most recently published [PCI DSS requirements](#). Language in the agreements should state that the third-parties agree to comply with PCI DSS security standards for the duration of their relationship with the University. Any contracted merchant that fails to be compliant during the term of its agreement with WLU will be deemed to have materially breached the agreement.

C. Internal Audit and Security Scan

WLU merchants should meet and maintain standards set forth in this policy based upon an annual review. This will include an internal audit and security scan under the direction of ITS, or select third-party with appropriate credentials. The purpose of this annual audit is to see that controls are in place and functioning as expected. This review will be based upon PCI DSS controls, and will be approved by the University's eCommerce Committee

- 1) Prior to initial implementation or usage of a payment system, a WLU merchant should undergo an internal audit conducted by the ISO. New entrants should be compliant with the WLU eCommerce Policy.
- 2) Thereafter, the ISO will audit the merchant's payment system and processes on an annual basis using the PCI DSS Security Audit Procedures. If the audit is not passed, the eCommerce Committee will suspend the WLU merchant's authorization to handle payment card and cardholder data.

D. Training

The ISO is the primary facilitator of PCI DSS compliance training. The University will engage in best practices identified by the PCI DSS, in addition to established WLU training guidelines that address eCommerce and credit card handling.

- 1) Prior to initial implementation or usage of a payment system, prospective WLU merchants should attend a training session facilitated by the ISO
- 2) Thereafter, on an annual basis, all WLU merchants should attend an annual eCommerce workshop facilitated by the ISO. If a merchant does not attend this workshop, the eCommerce Committee may suspend the merchant's authorization to handle payment card and cardholder data. During this workshop attendees will be asked to sign an agreement acknowledging their understanding of WLU's eCommerce Policy and Procedures

E. Requirements of a University Merchant

All WLU Merchants and their staff should adhere to the following requirements in order to achieve PCI DSS compliance. These are broadly summarized, however, the full listing of PCI DSS requirements can be found in section 4.2.1

- 1) All new payment systems that use internet connections should be tested, scanned, and approved by the ISO prior to their being moved into production.
- 2) If the WLU merchant's payment process involves paper forms, merchants should completely destroy the card validation value (CVV) and account number immediately after authorization by cross-cut shredding or incinerating. Concealment with a marker is not sufficient.
- 3) If a WLU merchant scans paper forms that contain cardholder data into an imaging system, the account number, CVV, and/or personal identification number (PIN) should be removed from the document or rendered unreadable prior to scanning, or redacted (not merely highlighted black) by a program that offers secure redacting (such as Adobe Acrobat Professional).
- 4) Merchants may not request or submit cardholder information via email or other insecure means. WLU merchants who receive unsolicited cardholder information should advise the sender of an appropriate way to make payments, but should take care to not include any cardholder information in any response.

- 5) WLU merchants should remove cardholder account numbers on receipts, reports, and other printed documents.
- 6) WLU merchants should physically store all paper-based cardholder information in a locked/secured location, with access allowed only on a need-to-know basis.
- 7) All cardholder data/records older than 18 months should be cross-cut shredded or incinerated. Passwords for payment systems and associated user accounts should be changed every 90 days. Compliance will be monitored by the ISO (See section 5 for details) and the Information Security Program Committee, as appropriate.
- 8) Third-party and WLU merchants should follow written guidelines and protocols specific to their payment system and related processes. Those guidelines and protocols may not be inconsistent with this eCommerce policy. WLU merchants should submit a copy of their policies/procedures to the eCommerce committee during the annual eCommerce audit.
- 9) Departments that have point-of-sale operations and locations where cardholder data is accessible should develop and follow procedures to help all personnel easily distinguish employees in those areas by assigning them ID badges. Procedures should be in place for granting new badges to employees (full-time, part-time, temporary and student workers), changing badge access, and revoking badges for terminated employees.
- 10) Employees, including student workers, whose job responsibilities involve access to cardholder data, should undergo criminal background checks prior to hire.
- 11) WLU merchants should notify ITS of the need to grant and maintain non-default, non-shared and unique individual accounts for each user of their payment system.
- 12) WLU merchants are responsible for notifying ITS of the need to modify or suspend the eCommerce account of any employee who changes employment role or leaves.
- 13) Sharing passwords is prohibited.
- 14) WLU merchants should maintain security controls consistent with PCI DSS requirements. This includes physically securing all paper, devices, and electronic media that contain payment card and/or cardholder information.
- 15) Management within a WLU merchant department must oversee, classify, and authorize all paper, electronic devices, and media that contain cardholder information during transportation. WLU merchants should establish procedures to classify such media as "confidential" as well as to track and log its distribution.
- 16) Paper forms should never request a recipient to write down his/her CVV or PIN.
- 17) WLU merchants will work with ITS to protect cardholder security through appropriate payment system configurations. This includes blocking users from administrative access to the underlying system.
- 18) If a payment system is not maintained by ITS, then the vendor must be PCI compliant.

- 19) Remote access by vendors to manage applications should be monitored and logged upon request from the merchant. These technologies should also automatically deactivate after 30 days of non-use. WLU merchants may not copy, move, or store cardholder data onto local hard drives or removable electronic media (e.g. electronic “thumb drives,” CDs, floppy disks, etc.).
- 20) Cardholder and Payment Card Data should reside on a segmented network.
- 21) A request from one of the charge card brands or the University’s acquiring bank should be processed in accordance with their rules and regulations.

F. Non-Compliance Penalties

The University may impose penalties upon WLU merchants in the event they do not comply with established policies, procedures, and controls. Such penalties will reflect the potential and/or actual damage to the school’s reputation and trust of its students, alumni, and business community in the event of a payment card breach at Washington and Lee. The cost for a data breach is expensive. Industry wide statistics show that in 2008, the cost per record breached was \$202.

Following are examples of potential costs that may be imposed upon the University and/or its merchants in the event of breach of cardholder data:

- 1) Fines imposed by acquiring bank and/or payment brand;
- 2) Costs to notify cardholders;
- 3) Credit Card replacement and remediation services for impacted cardholders;
- 4) Repayment of fraudulent charges that result from data breach;
- 5) Onsite forensics audit by a PCI-Qualified Data Security Company;
- 6) Merchant certification by a PCI-Qualified Data Security Company; and
- 7) Associated Legal Fees

G. Reporting a Data Breach

Even the best information security infrastructure cannot guarantee that intrusions or other malicious acts will not happen. The speed with which the University can recognize, analyze, and respond to an incident can limit the damage and lower the cost of recover

- 1) Any known or suspected breach in payment card or cardholder data should promptly be reported to the Office of General Counsel and the Chair of the Information Security Program Committee. The Incident Response Team should also be contacted if the breach involves electronic data.
- 2) The Information Security Program Committee will meet to determine the appropriate response and the timeline for taking responsive action. The Incident Response Team will be consulted on as needed basis on the nature of the breach.
- 3) The ISP Committee and/or the Incident Response Team, as applicable, will implement the business continuity and disaster policy and document communications related to the University’s response.

IV. ANNOTATED REVISION HISTORY

This policy has not yet been revised.
