FIN-037

Governance and Compliance Requirements for Payment Card Activities

Effective Date Thursday, August 3, 2017

Status Final

Last Revised Wednesday, April 7, 2021

Policy Type University

Contact Office University Payment Card Services

Oversight Executive
Vice President and Chief Financial Officer

Applies To Academic Division and the College at Wise.

Table of Contents

Reason for Policy

The University is committed to protecting cardholder data from loss or compromise. Consistent with that commitment, the University requires adherence to the Payment Card Industry Data Security Standards (PCI-DSS). In addition to protecting cardholder data, adherence to PCI-DSS reduces the likelihood of fines, penalties, and reputational damage to the University associated with data breaches.

The University's adherence to the PCI-DSS is a contractual requirement. This policy identifies the administrative offices responsible for establishing business processes for University units that process, store, or transmit cardholder data. Cardholder data are "highly sensitive data" subject to the security requirements of University policy and must be protected in accordance with all related University policies, standards, and procedures in addition to the PCI-DSS.

[Note: The aligned policy for the Medical Center is 0335, *Use of Payment Cards at the Medical Center*.]

Definition of Terms

Attestation of Compliance (AOC)

Description

Forms a merchant, service provider, or Qualified Security Assessor (QSA) may use to attest to the results of an annual Payment Card Industry Data Security Standards self-assessment**.**

Cardholder Data (CHD)

Description

Primary cardholder account number that identifies the issuer and a particular cardholder account, which can include cardholder name, expiration date, and/or service code.

Merchant

Description

A University unit that accepts payment cards (MasterCard, Visa, Discover, and American Express) as payment for goods or services. Merchant also includes any University-affiliated party that directly or indirectly accepts funds from payment cards under the University's merchant account managed by University Payment Card Services and has agreed to abide by applicable policies and associated procedures.

Merchant Account

Description

A unique identification number assigned to a merchant by MasterCard/Visa/Discover and American Express that binds the merchant to Payment Card Rules and Regulations.

Payment Card

Description

Credit cards and debit cards linked to the cardholder's account at a financial institution, e.g., an individual or an employer's business account.

Payment Card Industry (PCI) Data Security Standards (DSS)

Description

A robust security framework consisting of 12 baseline requirements for technical and operational controls pertaining to the protection of cardholder data. An annual attestation of compliance with the PCI-DSS is required for all entities involved in payment card processing.

Qualified Security Assessor (QSA)

Description

An individual who has been certified by the Payment Card Industry Security Standards Council to validate a merchant's or service provider's adherence to the Payment Card Industry Data Security Standards.

Report on Compliance (ROC)

Description

A survey tool used annually by eligible merchants and service providers to evaluate their compliance with the Payment Card Industry Data Security Standards.

Self-Assessment Questionnaire (SAQ)

Description

A survey tool used annually by eligible merchants and service providers to evaluate their compliance with the Payment Card Industry Data Security Standards.

Service Provider

Description

An entity, other than a card brand, that is directly involved in the processing, storage, or transmission of cardholder data on behalf of another entity. This includes entities that provide services that could impact the security of cardholder data.

University Payment Card Services (UPCS)

Description

An administrative unit within Financial Operations that oversees payment card activity for the Academic Division, the College at Wise, and under certain conditions, designated University-affiliated parties.

University-Affiliated Party

Description

An entity other than a unit of the Academic Division, the Medical Center, or the College at Wise authorized to collect funds under the University's merchant account network to support the University’s activities, units, or mission and that has agreed to comply with applicable University policy(ies). This may include but is not limited to University-Associated Organizations authorized to collect funds on behalf of the University.

Policy Statement

The use of payment cards to collect funds, whether received directly or through a third-party, requires review and approval by the appropriate University administrative offices before contracts are signed, merchant accounts are obtained, or revenue resulting from payment card processing is received. Additionally, any University-affiliated party authorized to collect funds on behalf of the University must abide by the requirements of this policy.

1. **Contract Review:**
   All contracts, including click-through end user license agreements (EULAs), with service providers that accept payment card payments on behalf of University units or activities must be signed by an authorized

signatory as described in University policy *FIN-036: Signatory Authority for Executing University Contracts*, and handled in accordance with *FIN-030: Purchases of Goods and Services* for the Academic Division and the College at Wise. This requirement applies whether or not the University is being charged for the service.

New or renewal contracts, including purchase orders, that currently include payment card processing or could include payment card processing by a unit of the Academic Division or the College at Wise or by a contracted third-party must include the latest version of the "Data Protection Addendum."

As part of the contract review process, the Procurement and Supplier Diversity Services "Buyer" (i.e., contract negotiator) will assure that the contract terms have been reviewed and approved by the University administrative office(s) responsible for Payment Card Industry Data Security Standards (PCI-DSS) compliance and information security.

2. **Business Process Approval and Merchant Requirements:**
All activities, equipment, and software used by a merchant that are related to payment card processing must be approved by University Payment Card Services (UPCS). Any subsequent addition or change to approved processes or equipment must also be reviewed and approved. Examples of additions or changes include but are not limited to:

   - Adding a new University-affiliated party for a University merchant account.
   - Adding, replacing, or upgrading a physical device used for payment card processing that has been previously approved by UPCS.
   - Changing merchant procedures that have been previously approved by UPCS.

   Merchants must comply with PCI-DSS, including but not limited to, completing an annual Self-Assessment Questionnaire (SAQ), Attestation of Compliance (AOC), or Report on Compliance (ROC) as appropriate. These requirements are a contractual obligation for any entity involved in payment card processing or who might receive revenue from payment card transactions.

   New or expanded revenue generating activities must be approved in accordance with University policy *FIN-049: Revenue Generating Activities* before payment cards are accepted or revenue received.

   All costs for transaction fees, website development (except as noted below), equipment, or operations associated with conducting these transactions will be borne by the merchant. In addition, the merchant will pay any fees and penalties associated with failure to comply with related University policies, standards, procedures, or the PCI-DSS.

   The merchant is responsible for collecting, reporting, and remitting sales tax in Virginia and certain other states in accordance with University policy *FIN-032: Collecting, Reporting, and Remitting Sales Tax*.

   Payment cards may be accepted only using methods authorized by UPCS.

   Note: Mobile payment processes through Class III personal devices (such as smart phones, tablets, PDAs, etc.) coupled with payment application (apps) or attached hardware (i.e.: Square®, Mobile Pay®, MobileMerchant ®, etc.) are not authorized for use at this time.

3. **Information Security Requirements:**
   Cardholder data are considered highly sensitive data and must be protected in accordance with all related University policies, standards, and procedures in addition to the PCI-DSS.

   Websites that include a payment processing component, pass cardholder data through to a payment page, or receive cardholder data that are returned from a payment page must be structured such that all website content resides on a PCI-DSS compliant web server. This requirement applies to UVA-hosted or managed web servers and to web servers hosted and managed by a contracted third-party.

   To maintain PCI-DSS security standards, merchants in the Academic Division and the College at Wise must use a UVA-managed payment landing page unless otherwise approved by UPCS.

   Note: UVA Finance centrally funds Information Technology Services - Custom Applications & Consulting Services (ITS-CACS) to develop basic payment landing pages for merchants in the Academic Division and College at Wise. Merchants may use the basic pages provided or contract directly with ITS-CACS for custom page or site development services with UPCS approval.

4. **University-Affiliated Parties:**
   Requests to accept payment cards by University-affiliated parties will be reviewed by UPCS and approved provided they agree to abide by the requirements of this policy and enter into an agreement with the University addressing PCI-DSS obligations.
5. **Review of Non-University-Affiliated Parties:**
   The University is contractually obligated to assure compliance with the PCI-DSS standards of a University-contracted vendor if it directs a customer to such vendor, even if the University does not directly benefit from the revenue. All non-University-affiliated parties that are collecting revenue from a University-related recommendation, must be approved by UPCS.

6. **Compliance with Policy:**
   Failure to comply with the PCI-DSS may result in suspension of the University's ability to accept payment cards as well as fines, penalties, and reputational damage. To confirm compliance with University policy and the PCI-DSS, the University reserves the right to suspend or terminate a merchant account number and/or a merchant's ability to process payment cards if the merchant's payment card activity creates significant institutional risk.

   The authority to suspend or terminate merchant activities resides with UPCS for the Academic Division, College at Wise, and University-Affiliated Parties.

   Failure to comply with the requirements of this policy may result in disciplinary action up to and including termination or expulsion in accordance with relevant University policies.

   Questions about this policy should be directed to University Payment Card Services.

Procedures

Payment Card Services (PCS): FAQs, Procedures, and Forms

Related Information

FIN-036: Signatory Authority for Executing University Contracts
IRM-002: Acceptable Use of the University's Information Technology Resources

IRM-003: Data Protection of University Information
IRM-004: Information Security of University Technology Resources
IRM-012: Privacy and Confidentiality of University Information

Medical Center Policy *Use of Payment Cards at the Medical Center*

Health System Policy HSG-002, Fundraising Oversight for UVA Health

Major Category Finance and Business Operations

Next Scheduled Review Sunday, March 21, 2027

Revision History

Removed a contact office and minor revisions to Section 2, 3 and 6 3/21/24; Updated & added new Section 5 4/7/21; Updated procedures 9/10/18; Updated contact office/procedures 4/19/18.

Category Cross Reference
Governance

Approved By Executive Vice President & Chief Operating Officer

Approved Date Thursday, August 3, 2017