RADFORD UNIVERSITY

Policy Title: Payment Cards Policy	**Effective Date: 5/5/2010**
Policy Number: FA-PO-1214	**Date of Last Review: 10/18/2018**
Oversight Department: Controller's Office	**Next Review Date: 10/1/2019**

1. PURPOSE

The *Payment Cards Policy* for Radford University (University) seeks to ensure compliance with the Payment Card Industry Data Security Standard (PCI DSS) through the implementation of appropriate controls for the secure handling and protection of cardholder data (CHD). The policy provides the steps that must be followed to request approval to accept payment cards or change the method(s) used for accepting payment cards, and establishes the requirements that must be followed in processing payment card transactions to reduce risks inherently associated with the handling of payment card transactions.

2. APPLICABILITY

The *Payment Cards Policy* applies to all University merchants and persons who, on behalf of the University, accept payment cards and/or handle electronic or paper documents associated with payment card transactions.

3. DEFINITIONS

Cardholder: A person or organization to whom a payment card is issued or any person authorized to use the payment card.

Cardholder Data (CHD): Consists, at a minimum, of the full primary account number (PAN). Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date, and/or service code. Cardholder data must be protected.

- **Primary Account Number (PAN):** The unique payment card number that identifies the issuer and the particular cardholder account. Also referred to as "account number".
- **Cardholder Name:** The name of the cardholder to whom the card has been issued.
- **Expiration Date:** The date after which a card expires and is no longer valid. The expiration date is embossed, encoded, or printed on the card.
- **Service Code:** A three-digit or four-digit value in the magnetic stripe that follows the expiration date of the payment card on the track data. It is used for various purposes, for example, defining service attributes or identifying usage restrictions).

Cardholder Data Environment (CDE): The people, processes, and technology that store, process, or transmit cardholder data or sensitive authentication data.

Merchant: Any University department, office, or other entity authorized by the Associate Vice President for Finance and University Controller to accept payment card transactions on behalf of the University.

Merchant Account: A type of bank account that allows businesses to accept payments by payment card. A merchant account is established under an agreement between an acceptor and a merchant acquiring bank for the settlement of payment card transactions.

Payment Card: For purposes of this policy and compliance with the PCI DSS, any payment card/device that bears the logo of the founding members of the PCI Security Standards Council, which are American Express, Discover Financial Services, JCB International, MasterCard Worldwide, or Visa, Inc.

Payment Card Industry Data Security Standard (PCI DSS): A baseline of technical and operational requirements designed to protect cardholder data. PCI DSS applies to all entities involved in payment card processing, as well as entities that store, process or transmit cardholder data (CHD) and/or sensitive authentication data. The standard applies to CHD in any format including electronic and paper formats. PCI DSS was developed by the Payment Card Industry Security Standards Council (PCI SSC).

The PCI SSC is an open global forum, launched in 2006 by five global payment brands -- American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc., that is responsible for the development, management, education, and awareness of the PCI Security Standard, including the Data Security Standard (PCI DSS). The Council's five founding brands have incorporated the PCI DSS as the technical requirements of each of their data security compliance programs. Further details can be found at the PCI Security Standards Council Web site (https://www.pcisecuritystandards.org).

Payment Card Transactions: Financial transactions that use cardholder data related to payment cards whether processed by facsimile, paper, card presentation, or electronic means.

PCI Compliance Steering Committee: An operational committee, established under this policy, to serve in an advisory capacity to the Associate Vice President for Finance and University Controller in monitoring the University's cardholder data environment (CDE) to ensure compliance with PCI DSS (see Charter in Appendix A).

Sensitive Authentication Data: Security-related information used to authenticate cardholders and/or authorize payment card transactions. This information must be properly protected if stored before the transaction is run, but must never be retained after transaction authorization regardless of the success or failure of the transaction. This information includes, but is not limited to:

- **Magnetic stripe (Track) data:** Data encoded in the magnetic stripe or chip used for authentication and/or authorization during payment transactions.
- **CAV2, PAN CVC2, CID, or CVV2 data:** The three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card-not-present transactions.

- **PIN:** Acronym for personal identification number, which is a secret numeric password known only to the user and a system to authenticate the user to the system. The user is only granted access if the PIN the user provided matches the PIN in the system.
- **PIN block:** A block of data used to encapsulate a PIN during processing. The PIN block format defines the content of the PIN block and how it is processed to retrieve the PIN. The PIN block is composed of the PIN, the PIN length, and may contain subset of the PAN.

University Payment Card Coordinator: The Bursar is designated as the University Payment Card Coordinator.

4. POLICY

A. The acceptance of payment cards as a form of payment for any University activity must have the **prior written approval** of the Associate Vice President for Finance and University Controller (AVPF/UC). Without such approval, University departments, offices, employees, or other persons do not have the authority to contract for or use, in any manner, payment card services in collecting funds related to any University activity.

B. Merchants accepting payment cards related to any University activity must do so in compliance with the PCI DSS and this policy.

C. Merchants must not use any of the University's affiliated foundations to process payment card transactions except for gifts and donations that are legitimately deposited with the affiliated foundations.

D. Merchants are responsible for all costs associated with the installation and maintenance of providing payment card services.

E. Merchants accepting payment card transactions over the internet must use third-party service providers for processing payment card transactions to mitigate risk to the University. All websites developed to process payment card transactions must be structured in such a way as to ensure the University's web server(s) are not brought into scope for PCI compliance.

F. Third-party service providers must be certified as being PCI DSS compliant. In situations where proper documentation of compliance with PCI DSS cannot be obtained, both prior to implementation and annually thereafter, the AVPF/UC, in consultation with the PCI Compliance Steering Committee and the Information Security Officer, may apply a risk-based approach in reviewing other documentation in support of a decision to approve or disapprove the use of a third-party service provider.

G. Merchants must ensure administrative and information technology security procedures are developed and maintained in relation to their payment card operations that will ensure compliance with PCI DSS and this policy.

H. Prior to performing any payment card related responsibilities, **all** persons involved in accepting, processing, or reconciling payment card transactions on behalf of the University must read this policy, complete training provided or coordinated by the Controller's Office on the secure handling of payment cards and payment card transactions, and sign a Payment Card Security and Confidentiality Agreement (see Appendix C). Training must be completed annually.

I. The AVPF/UC must ensure that a validation of compliance with PCI DSS is performed annually, which will be coordinated by the University Payment Card Coordinator. Merchants must fully cooperate as directed in the annual validation of compliance.

J. Merchants are responsible for any fines levied against the University that result from non-compliance with PCI DSS by the merchant or any person authorized to process payment card transactions on behalf of the merchant.

K. All persons who have access to cardholder data on behalf of the University must protect that information in compliance with established policies and procedures, including PCI DSS.

L. Payment card processing privileges may be revoked if a merchant fails to comply with the PCI DSS and/or this policy. Any person who fails to accept and process payment cards in accordance with established policies and procedures, including PCI DSS and this policy, may be subject to disciplinary action, as applicable, in addition to criminal and civil penalties imposed by law.

5. PROCEDURES

A. Requests for Approval to Accept Payment Cards or Change the Method(s) of Processing Payment Cards

1. The *Request to Accept Payment Cards* form (see Appendix B) must be submitted to accept payment cards for goods or services or change the method(s) of processing payment cards. Proper advance planning is crucial for ensuring compliance with all aspects of PCI DSS. Therefore, requests must be submitted **as early as possible, but not less than three months in advance** of the desired date to begin accepting payment cards.

2. All *Request to Accept Payment Cards* forms will be reviewed by the PCI Compliance Steering Committee to identify potential areas of concern related to compliance with PCI DSS. The PCI Compliance Steering Committee will advise the AVPF/UC on any issues that need to be resolved prior to approving the request. A detailed review of the proposed business processes and measures proposed to ensure compliance with PCI DSS may be required prior to approval.

3. The AVPF/UC will approve or disapprove the request and notify the department head who approved the request.

B. Procurement and Contractual Requirements

1. Any software applications, third-party services, payment channels, etc., for the acceptance of payment cards must be procured in accordance with procurement policies and procedures as detailed in the Radford University Procurement and Contracts Procedures Manual.

2. Prior to finalizing any purchase or signing any contracts related to the items in Section 4.B.1. above, documentation must be obtained attesting to the product's or service's compliance with PCI DSS. Request for proposal's (RFPs) must include a requirement that this documentation be submitted as part of the proposal. The following (listed in order of preference) are considered valid forms of documentation and must be less than 12 months old:

a. A valid Attestation of Compliance (AOC) completed by a Qualified Security Assessor (QSA)

b. A screen print from the Visa Global Listing of Service Providers website showing the service provider as approved.

3. Additionally, any third-party contracts must include contractual language requiring the contractor's compliance with PCI DSS. Such contractual language will be provided by the Office of Procurement & Contracts in consultation with the AVPF/UC.

4. Thereafter, merchants must obtain and submit annual attestations of PCI DSS compliance as referenced in Section 5.B.2. above. Copies of the attestations must be provided to the University Payment Card Coordinator as requested.

5. In situations where the University must make arrangements directly with a vendor for payment card merchant processing services, as opposed to a hosted service that includes these services with payment remitted to the University, the Virginia Department of Treasury's merchant card contract must be used. Any exceptions must be approved by the AVPF/UC. The AVPF/UC, or designee, will submit the appropriate forms to the Virginia Department of Treasury to establish required merchant accounts.

C. <u>Handling and Processing of Payment Cards Requirements</u>

1. Cardholder data must be handled in compliance with the following requirements:

a. Merchants must not, under any circumstances, store in any form sensitive authentication data (e.g. magnetic stripe/track data, CVV2/CVC2, PIN, etc.) subsequent to authorization, even if encrypted.

b. Access to cardholder data must be restricted to only those persons who need the data to perform their jobs, have been properly trained, and have signed a Payment Card Security and Confidentiality Agreement.

c. Cardholder data, whether processed on paper or electronically, must be protected from unauthorized access until processed by storing them in locked cabinets or non-portable safes dedicated solely to these records. All stored information or records must be marked confidential and be properly disposed of as soon as the transactions have been processed.

d. All equipment and systems used to process cardholder data must be secured against tampering and unauthorized access or use. Persons responsible for processing payment cards must be constantly aware of their equipment and systems. Payment card processing equipment must not be left unattended without being properly secured.

e. Persons responsible for processing payment cards must regularly inspect equipment to ensure there is no evidence of tampering in accordance with departmental procedures (see Appendix D). The inspections must be documented in a log (see Appendix E).

f. Email must never be used to transmit cardholder data and may never be accepted as a method to supply such information. If a customer does email cardholder data, the merchant must respond to the email, first removing any cardholder data that was

included, and inform the customer that, in the interest of payment card security, the payment cannot be processed based on the email. Provide any other necessary information or instructions as directed by your supervisor.

g. Fax machines used to transmit cardholder data to a merchant must be connected to an analog phone line and not to the internet or University network. Additionally, the fax machines must not have the capability of storing data to a hard drive (e.g. multi-functional devices). Fax machines that are used for payment card processing must be protected from tampering and unauthorized access or use.

h. Cardholder data must not be retained any longer than the period for which there is a documented business, legal, or regulatory purpose; after which, the data must be deleted or destroyed. Paper or hard copy records must be destroyed by cross-cut or micro-cut shredding. For electronic records, consult with the Division of Information Technology (DoIT) for proper methods of deleting records.

2. All revenue generated through payment cards handled by the merchant must be deposited and reconciled daily in accordance with the *Funds Handling Policy*. In situations where a third-party contractor is handling the processing of payment card transactions under contract with the University, payment from the contractor must be received at least monthly. When received, such payments are then subject to the *Funds Handling Policy*.

3. When an item or service is purchased using a payment card and a refund is necessary, the refund must be credited to the same payment card account from which the purchase was made. There must be adequate separation of duties between the person issuing a refund and the person reconciling the payment card transaction.

D. Oversight and Recordkeeping

1. Merchants must designate a full-time employee as the Merchant Payment Card Coordinator, who has primary authority and responsibility for oversight for payment card and/or e-commerce transaction processing and ensuring compliance with this policy. The Merchant Payment Card Coordinator is also responsible for ensuring all persons processing payment card transactions for the merchant area complete the annual PCI DSS training and sign the Payment Card Security and Confidentiality Agreement as required. Changes to the person serving in this role must be reported to the University Bursar immediately.

2. Merchants must develop and maintain current written procedures covering administrative and information technology responsibilities that will ensure compliance with the PCI DSS. Guidelines for preparing written procedures are included in Appendix D. Procedures must be approved in writing by the respective department head and provided to the University Payment Card Coordinator upon request.

3. Merchants must maintain a current log of all persons with access to cardholder data. At a minimum, the document should list the name, the date annual training was last attended, a verification that each person has read this policy and been trained on internal procedures, and the date the Payment Card Security and Confidentiality Agreement was last signed. Documentation may be maintained in the written procedures (see Appendix D) or in a separate log (see sample log in Appendix F). The log must be reviewed monthly

by the respective department head, or designee, to ensure that the log reflects the most current information. Documentation of the monthly review must be retained in the merchant's files.

4. Signed Payment Card Security and Confidentiality Agreements must be maintained and readily accessible for each person presently authorized to process payment cards on behalf of the University. Signed agreements for persons no longer employed by the merchant may be maintained separately and should be disposed of in accordance with applicable record retention requirements.

5. Merchants must maintain a current log of all equipment used for payment card processing. Documentation may be maintained in the written procedures (see Appendix D) or in a separate log. The log must be reviewed monthly by the Merchant Payment Card Coordinator to ensure that the log reflects the most current information. Documentation of the monthly review must be retained in the merchant's files.

6. Merchants must maintain a current log of all third-party service providers involved in payment card processing including payment gateways and merchant processors. Documentation may be maintained in the written procedures (see Appendix D) or in a separate log.

E. Reporting Suspected Security Events or Fraud

1. Any person that suspects a security breach has occurred related to payment cards or payment card transactions must immediately notify the University's IT Security Office at itsecurity@radford.edu and must follow instructions provided by that office.

2. The Information Security Officer will immediately contact appropriate University and other officials as required under the circumstances.

3. Merchants and all persons responsible for processing payments cards must provide the utmost cooperation and assistance, as required, in any investigation of a suspected security breach.

4. Any person that suspects fraudulent activity related to payment card transactions must immediately report the matter in accordance with the University's *Fraud, Waste, and Abuse Policy*.

6. EXCLUSIONS

This policy does not apply to student clubs and organizations whose financial activity is not accounted for through the University's financial system.

7. APPENDICES

Appendix A: PCI Compliance Steering Committee Charter

Appendix B: Request to Accept Payment Cards

Appendix C: Payment Card Security and Confidentiality Agreement

Appendix D: Guidelines for Preparing Written Payment Card Processing Procedures

Appendix E: Card Reader Tamper Inspection Log

Appendix F: Payment Card Processing - Authorized Employees Log

8. REFERENCES

Payment Card Industry Data Security Standard (PCI DSS)

9. INTERPRETATION

The authority to interpret this policy rests with the President of the University and is generally delegated to the Vice President for Finance and Administration & Chief Financial Officer.

10. APPROVAL AND REVISIONS

The original version of this policy, *Policy on Payment Cards*, was approved by the Vice President for Finance and Administration on May 5, 2010.

The newly developed *Payment Cards Policy* was submitted to and approved by the President's Cabinet at the meeting held on November 5, 2014. President Kyle signed the *Payment Cards Policy* on November 11, 2014.

Effective July 1, 2017, the *Payment Cards Policy* was reviewed by the oversight department, the PCI Compliance Steering Committee, and the Office of Policy Compliance. Minor revisions were made, but no substantive changes were made that would alter the scope or application of the policy.

Effective October 18, 2018, the *Payment Cards Policy* was reviewed by the oversight department and the Office of Policy Compliance. Revisions were made to the procedures, but only minor editorial changes were made to two policy statements, which did not alter the scope or application of the policy. The Vice President for Finance and Administration & Chief Financial Officer approved the revisions on October 18, 2018.

For general information concerning University policies, contact the Office of Policy and Tax Compliance – (540) 831-5794. For questions or guidance on a specific policy, contact the Oversight Department referenced in the policy.