Policy Title: Payment Cards Policy	Effective Date: 5/5/2010

- **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

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. Handling and Processing of Payment Cards Requirements

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

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 reviewe0.2di002 Tc2.8 (r)-6 (r)-2y2 Tw 7.ni pala -0.8 (y)-7.5 ( )1-5.

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