I. **Policy Statement:** Towson University is committed to reduce institutional risk associated with the acceptance of payment cards by establishing and adopting standard payment systems and clear assignment of responsibility. This policy provides campus departments with PCI Standard-compliant, reliable and supportable methods for securely and conveniently accepting card payments and establishing a process for formally evaluating the need for payment systems outside the scope of the commonly supported methods. This policy applies when Towson University or its third party service providers accept a payment via a payment card. It does not apply when the University uses a payment card to acquire goods and/or services.

II. **Definitions:**

A. **PCI Standard** – The Payment Card Industry Standard is the result of collaboration among the major credit card brands to develop a single approach to safeguarding sensitive data. The PCI Standard defines a series of best practices for handling, transmitting and storing sensitive data.

B. **Cardholder Data** – Cardholder Data is any personally identifiable data associated with a cardholder, including an account number, the full primary account number (PAN), card type, expiration date, PIN, name, address, social security number, or Card Validation Code (e.g., three-digit or four-digit value printed on the front or back of a payment card (e.g., CVV2 and CVC2 data)).

C. **Credit Charge Merchant** – any person, department, or entity within the University accepting payment for goods or services (including conference registrations, memberships, fees, etc.) via a payment card.

D. **Third-party Service Provider** – Any entity the University contracts with that has access to Cardholder Data in order to carry out its obligations.

III. **Responsible Executive and Office:**

Responsible Executive: Vice President for Administration & Finance and Chief Financial Officer (CFO)

Responsible Office: Financial Affairs
IV. Entities Affected by this Policy:

This policy applies to all Towson University departments, entities and employees that accept and process, transmit, or handle cardholder information in any format or contract with a third party for services that include payment cards. All computers and devices at Towson University involved in processing payment card data are required to comply with card security standards as established by the Payment Card Industry (PCI) Security Standards Council.

V. Procedures:

A. All transactions involving credit card information to, from, or on behalf of the University must be performed via processes approved by the Payment Card Committee (PCC). Departments involved with the acceptance of and processing of credit cards for payment of goods and services must design adequate processes in compliance with the procedures on the PCC website. All systems that have been approved for card acceptance activity must be administered in accordance with the requirements of all applicable University policies.

B. The PCC shall maintain a website with relevant payment card security information, forms, and contact information. The PCC may amend the procedures from time to time without the need to amend this policy.

C. Payment Card Committee

1. The University has established the Payment Card Committee (PCC) to administer and oversee payment card use. The committee will include, but is not limited to, representatives from Financial Affairs and OTS.

2. The PCC shall review all proposed business plans involving credit card sales over the internet. The Committee will review each proposal for intended business purpose, consistency with the University's mission and policies, and selling department’s ability to support card activity.

3. Utilization of existing solutions that comply with this policy will be required. In special cases, alternative solutions will be considered after a comprehensive review. The PCC will consider exceptions on a case-by-case basis in consultation with the Office of Technology Services’ Information Security and the Office of Management Advisory and Compliance Services. In considering exceptions, the PCC will examine compliance with applicable standards and the existence and reliability of compensating controls.

4. Following review and approval, the PCC will notify the requesting department of approval status, determine the appropriate accounts and revenue
object codes to be credited for sale proceeds, and issue a unique merchant ID identifier for the selling department.

5. Any changes to approved payment processes that affect compliance with this policy must be reviewed and approved by the PCC prior to implementation. Proposed changes should be routed to the PCC.

6. The PCC shall oversee the University’s efforts to comply with this policy, including but not limited to documenting required annual assessments and training.

D. Sanctions

Departments not complying with this policy may lose the privilege to serve as a Credit Card Merchant. Additionally, fines may be imposed by the affected credit card company, and the non-compliant department will be responsible for paying such fees. Persons in violation of this policy are subject to the full range of sanctions, including but not limited to termination of employment. The University will carry out its responsibility to report such violations to the appropriate authorities.

Related Policies:

Approval Date: 09/06/2017

Effective Date: 09/06/2017

Approved by: President’s Council 09/06/2017